J. Math. Soc. Japan
Vol. 64, No. 1 (2012) pp. 23–85
doi: 10.2969/jmsj/06410023

The cuspidal class number formula for the modular curves $X_1(2p)$

By Toshikazu Takagi

(Received June 22, 2010)

Abstract. Let p be a prime not equal to 2 or 3. We determine the group of all modular units on the modular curve $X_1(2p)$, and its full cuspidal class number. We mention a fact concerning the non-existence of torsion points of order 5 or 7 of elliptic curves over $\boldsymbol{Q}$ of square-free conductor n as an application of a result by Agashe and the cuspidal class number formula for $X_0(n)$. We also state the formula for the order of the subgroup of the $\boldsymbol{Q}$-rational torsion subgroup of $J_1(2p)$ generated by the $\boldsymbol{Q}$-rational cuspidal divisors of degree 0.

1. Introduction.

Let X be a modular curve. Let S be a subset of the set S_c of all cusps on X, and let C_S be the subgroup of the divisor class group of X consisting of the classes of divisors of degree 0 which are supported on S. (The group C_{S_c} is called the cuspidal divisor class group of X.) Kubert and Lang [**7**] considered the problem to determine if C_{S_c} is finite, and when it is finite to compute its order. (The order of C_{S_c} is called the cuspidal class number of X.) Manin [**8**] and Drinfeld [**4**] had already proved the finiteness of C_{S_c}, but their method gave no information about the order. Kubert and Lang [**7**] found an altogether different proof of the Manin-Drinfeld theorem in which the whole point was to exhibit the group of modular units on the modular curve X. (A function on X is called a modular unit on X if its divisor is supported on S_c.) In the case $X = X(n)$ where n is a power of a prime $p \neq 2, 3$, Kubert and Lang [**7**] could determine the cuspidal class number of $X(n)$. Kubert and Lang [**7**] also considered the case where n has more prime factors than one, but there was an essential difficulty. In the case where n is a power of a prime, the group of the modular units is generated by special functions called Siegel units. But when n has more prime factors than one, the group of the modular units contains square roots of Siegel units, and because of this fact

2010 *Mathematics Subject Classification.* Primary 11G18; Secondary 11F03, 11G05, 14G05, 14G35, 14H40, 14H52.

Key Words and Phrases. modular curve, modular unit, cuspidal class number, elliptic curve, Jacobian variety, torsion subgroup.

the cuspidal class number was not determined. (For this fact, see Kubert [**6**] and Stevens [**12**]).

When X is a modular curve of other type, several authors have considered its cuspidal class number.

Let $X = X_0(n)$. Ogg [**10**] determined the case where n is a prime, and Takagi [**16**] determined the case where n is square-free. Also, Takagi [**19**] computed the cuspidal class number of a curve which is a quotient of $X_0(n)$ with n square-free by Atkin-Lehner involutions.

Let $X = X_1(n)$. In this case, firstly Klimek [**5**] considered the subgroup C_S of C_{S_c} where S is the set S_0 of 0-cusps under the assumption that n is a prime, and computed its order. (A cusp on $X_1(n)$ is called a 0-cusp if it lies over the cusp 0 of the curve $X_0(n)$.) Kubert and Lang [**7**] also considered the subgroup C_{S_0} in the case where n is a power of a prime $p \neq 2, 3$. Lastly, Yu [**21**] computed the order of the subgroup C_{S_0} in the case where n is an arbitrary integer. (Note that there is a misprint in the formula of [**21**], which is corrected in Yang [**20**].)

As to the full cuspidal class number of $X_1(n)$, Takagi [**13**] determined the case where n is a prime, and Takagi [**14**], [**15**], [**17**] determined the case where n is a power of a prime with the exception of the case where n is an even power of 2.

The purpose of the present paper is to consider the modular curve $X_1(n)$ in the case where n has more prime factors than one. In fact, we consider the case $n = 2p$ with p a prime as a first step. In view of the case of $X(n)$ with n having more prime factors than one, it seems possible that the group of the modular units contains square roots of Siegel units. But, fortunately, our study reveals that it is not the case at least in the case $n = 2p$, therefore, we can compute the cuspidal class number of $X_1(2p)$.

One of our main results is the determination of the group of the modular units on $X_1(2p)$, which is given in Theorem 4.2. The other main result is the description of the cuspidal class number of $X_1(2p)$ (Theorem 5.2), which is given as follows.

Main Theorem. *Let p be a prime $\neq 2, 3$. Let h be the cuspidal class number of the modular curve $X_1(2p)$. Then we have*

$$h = \frac{p^2-1}{24} \cdot p^2 \cdot \prod_{\psi} \left\{ (4-\psi(2))^2 \left(\frac{1}{4} B_{2,\psi} \right)^4 \right\},$$

where ψ runs through all even, primitive Dirichlet characters modulo p.

In the theorem above, the symbol $B_{2,\psi}$ denotes the generalized Bernoulli number relative to ψ defined by

$$B_{2,\psi} = p\sum_{a=1}^{p-1}\psi(a)B_2\left(\frac{a}{p}\right)$$

with $B_2(X) = X^2 - X + 1/6$ (the second Bernoulli polynomial).

The study of the cuspidal divisor class group plays an important role in the area of the arithmetic of the Jacobian variety of a modular curve. Let X be a modular curve. Let $i_\infty : P \mapsto [(P) - (\infty)]$ be the cuspidal embedding of X into its Jacobian J_X sending a point P to the divisor class of $(P) - (\infty)$. When P is a cusp on X, the point $i_\infty(P)$ is a torsion point on J_X.

Let $X = X_0(n)$. Then X has a $\boldsymbol{Q}$-rational model, which is defined by the property that its function field is the field of modular functions for $\Gamma_0(n)$ whose Fourier coefficients belong to $\boldsymbol{Q}$. The cusp ∞ is a $\boldsymbol{Q}$-rational point of $X_0(n)$. In particular, when n is square-free, all cusps on $X_0(n)$ are $\boldsymbol{Q}$-rational points of $X_0(n)$. Therefore, the cuspidal divisor class group is a $\boldsymbol{Q}$-rational torsion subgroup of $J_0(n)$ $(= J(X_0(n)))$. When n is a prime p, Ogg [**11**] conjectured and Mazur [**9**] proved that the full $\boldsymbol{Q}$-rational torsion subgroup of $J_0(p)$ is the cuspidal divisor class group.

Let n be square-free. Let A be an elliptic curve over $\boldsymbol{Q}$ of conductor n. Let r be a prime that does not divide $6n$. Agashe [**1**] proved that if r divides the order of the $\boldsymbol{Q}$-rational torsion subgroup $A(\boldsymbol{Q})_{tor}$ of $A(\boldsymbol{Q})$, then r divides the order of the cuspidal divisor class group of $X_0(n)$. By [**9**], the only primes that can divide the order of $A(\boldsymbol{Q})_{tor}$ are 2, 3, 5 and 7. Therefore, the possible value of r is 5 or 7 with $r \nmid n$. On the other hand, by the formula for the cuspidal class number of $X_0(n)$ in [**16**, Theorem 5.1], we can see that r divides the cuspidal class number of $X_0(n)$ if and only if at least one prime factor p of n satisfies $p \equiv \pm 1 \pmod{r}$.

Combining the result by Agashe [**1**] with that by [**16**, Theorem 5.1], we obtain immediately the following theorem.

THEOREM. *Let n be a square-free integer. Let A be an elliptic curve over $\boldsymbol{Q}$ of conductor n.*

(1) *Assume that every prime factor p of n satisfies $p \not\equiv 0, \pm 1 \pmod 5$. Then A has no $\boldsymbol{Q}$-rational point of order* 5.
(2) *Assume that every prime factor p of n satisfies $p \not\equiv 0, \pm 1 \pmod 7$. Then A has no $\boldsymbol{Q}$-rational point of order* 7.

Let $X = X_1(n)$. Then X has a $\boldsymbol{Q}$-rational model, which is defined by the property that its function field is the field of modular functions for $\Gamma_1(n)$ whose Fourier coefficients belong to $\boldsymbol{Q}$. The ∞-cusps are $\boldsymbol{Q}$-rational points of $X_1(n)$. (A cusp on $X_1(n)$ is called an ∞-cusp if it lies over the cusp ∞ of the curve $X_0(n)$.) Therefore, the group C_S where S is the set S_∞ of ∞-cusps is a $\boldsymbol{Q}$-rational torsion subgroup of $J_1(n)$ $(= J(X_1(n)))$. The order of the group C_{S_∞} is equal to that of the group C_{S_0} which is known by [**5**], [**7**] and [**21**]. In the case where n is a prime $p \neq 2, 3$, Conrad, Edixhoven and Stein [**3**, Conjecture 6.2.2.] conjectured that the full $\boldsymbol{Q}$-rational torsion subgroup of $J_1(p)$ is the group $C_{S\infty}$, and verified it for a few cases of p.

In order to study the $\boldsymbol{Q}$-rational points in the cuspidal divisor class group, it is necessary to consider the $\boldsymbol{Q}$-rational cuspidal divisors of degree 0. In the case where n is a prime $p \neq 2, 3$, Chen [**2**] proved that the subgroup of $J_1(p)$ generated by the classes of $\boldsymbol{Q}$-rational cuspidal divisors of degree 0 coincides with $C_{S\infty}$. In some cases where n is not a prime, there occur $\boldsymbol{Q}$-rational cusps which are not ∞-cusps.

Let $n = 2p$ with p a prime $\neq 2, 3$. In this case there exist $\boldsymbol{Q}$-rational cusps which are not ∞-cusps. If a cusp P of $X_1(2p)$ is represented by a/c $(\in \boldsymbol{Q} \cup \{\infty\})$ with $(a, c) = 1$ and $(c, 2p) = 2p/r$, we say that P is of type r. The ∞-cusps are the cusps of type 1. The cusps of type 2 are also $\boldsymbol{Q}$-rational. The cusps of type p or $2p$ are not $\boldsymbol{Q}$-rational, therefore the subgroup $C_{(1,2)} = C_S$ of C_{S_c} with S the set of cusps of type 1 or 2 coincides with the subgroup of $J_1(2p)$ generated by all $i_\infty(P)$ with P a $\boldsymbol{Q}$-rational cusp. In addition to the $\boldsymbol{Q}$-rational cusps, there exist $\boldsymbol{Q}$-rational cuspidal divisors of degree 0. Put $D_{(2p)} = \sum_{x \in A_1} \{(1/x) - (\infty)\}$ and $D_{(p)} = \sum_{x \in A_2} \{(1/2x) - (\infty)\}$, where A_1 (respectively A_2) denotes a complete set of representatives of $(\boldsymbol{Z}/2p\boldsymbol{Z})^\times/\{\pm 1\}$ (respectively $(\boldsymbol{Z}/p\boldsymbol{Z})^\times/\{\pm 1\}$). These are $\boldsymbol{Q}$-rational divisors of degree 0. Put $C_{\boldsymbol{Q}} = C_{(1,2)} + \boldsymbol{Z}[D_{(2p)}\ ] + \boldsymbol{Z}[D_{(p)}]$. Then $C_{\boldsymbol{Q}}$ coincides with the subgroup of $J_1(2p)$ generated by the classes of $\boldsymbol{Q}$-rational divisors of degree 0. Continuing the arguments in the present paper, we can prove the following statement, and also determine the p-primary part of $C_{\boldsymbol{Q}}$. However, those results and proofs will be given in other papers.

Statement. *Let p be a prime $\neq 2, 3$. Let $C_{(1,2)}$ and $C_{\boldsymbol{Q}}$ be the subgroups of $J_1(2p)$ defined above.*

(1) $C_{\boldsymbol{Q}} = C_{(1,2)}$.
(2) *Let $h_{\boldsymbol{Q}}$ be the order of $C_{\boldsymbol{Q}}$. Then we have*

$$h_{\boldsymbol{Q}} = \frac{p^2 - 1}{24} \cdot p \cdot \prod_{\psi} \left\{ (4 - \psi(2)) \left(\frac{1}{4} B_{2,\psi} \right)^2 \right\},$$

where ψ runs through all even, primitive Dirichlet characters modulo p.

In the following we describe the contents of each section. In Section 2 we consider the modular curve $X_1(M)$ with M square-free. Here we parametrize the set of cusps by an abelian group called a Cartan group, and identify the cuspidal divisor group with the group ring of the Cartan group. In particular some relations between the divisors of Siegel functions are proved. In Section 3 we confine the study to the case $M = 2p$. The purpose of this section is to prove that the group of modular units is generated by Siegel functions. In Section 4 we determine the group of modular units. In Section 5 we compute the cuspidal class number.

In the present paper we denote by $\boldsymbol{N}$, $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$, $\boldsymbol{C}$, 1_2 the set of natural numbers, the ring of rational integers, the field of rational numbers, the field of real numbers, the field of complex numbers, the two-by-two identity matrix, respectively.

2. Modified Siegel functions on the curves $X_1(M)$.

In this section we consider modular curves $X_1(M)$ with M square-free, and construct modular units on $X_1(M)$ by the use of modified Siegel functions. We parametrize the cusps of $X_1(M)$ by an abelian group (called a Cartan group), and identify the cuspidal divisor group with its group ring. In order to do it, we consider a conjugate of the group $\Gamma_1(M)$ which is a principal congruence subgroup of $G(\sqrt{M})$. In general, the cusps of the curve determined by a principal congruence subgroup of $G(\sqrt{M})$ can be parametrized by an abelian group. This fact was used in our previous papers [**13**]–[**15**] and [**17**], and proved in [**18**] for arbitrary principal congruence subgroups of $G(\sqrt{M})$.

2.1. Modular curves $X_1(M)$ and X_I.

Let Γ be a Fuchsian group of the first kind. We denote by X_Γ the complete nonsingular curve associated with the quotient space $\Gamma\backslash\mathfrak{H}$, where the symbol $\mathfrak{H}$ denotes the upper half plane.

Let M be a square-free integer fixed throughout this section with $M \neq 1$. We denote by $\Gamma_1(M)$ the subgroup of $SL_2(\boldsymbol{Z})$ consisting of all matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ $(\in SL_2(\boldsymbol{Z}))$ with $a - 1 \equiv d - 1 \equiv c \equiv 0 \pmod{M}$. When $\Gamma = \Gamma_1(M)$, we denote the curve X_Γ by $X_1(M)$.

Let T be the set of all positive divisors of M, and regard it as a group with the product defined by $r \circ s = rs/(r,s)^2$ where (r,s) denotes the greatest common divisor of r and s $(r, s \in T)$. Let $\mathscr{O}$ be the order defined by $\mathscr{O} = \sum_{r \in T} \boldsymbol{Z}\sqrt{r}$. We denote by $G(\sqrt{M})$ the subgroup of $SL_2(\mathscr{O})$ consisting of all elements α of the form

$$\alpha = \begin{pmatrix} a\sqrt{r} & b\sqrt{r^*} \\ c\sqrt{r^*} & d\sqrt{r} \end{pmatrix}, \tag{2.1}$$

where $a, b, c, d \in \boldsymbol{Z}$, $r \in T$ and $r^* = M/r$. We call r the *type* of α, and denote it by $t(\alpha)$. Let I be the ideal of $\mathscr{O}$ defined by $I = \sqrt{M}\mathscr{O}$. We denote by $\Gamma(I)$ the subgroup of $G(\sqrt{M})$ consisting of all elements α satisfying

$$\alpha \equiv 1_2 \pmod{I}, \tag{2.2}$$

and call it a *principal congruence subgroup* of $G(\sqrt{M})$. When $\Gamma = \Gamma(I)$, we denote the curve X_Γ by X_I.

We have

$$\Gamma(I) = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{M} \end{pmatrix}^{-1} \Gamma_1(M) \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{M} \end{pmatrix}. \tag{2.3}$$

Hence the curve $X_1(M)$ is isomorphic to the curve X_I.

2.2. The function field of the curve X_I.

We denote by $\mathfrak{F}_I$ the field of all automorphic functions with respect to the group $\Gamma(I)$ such that their Fourier coefficients belong to the cyclotomic field $k_M = \boldsymbol{Q}(e^{2\pi i/M})$, and by $\mathfrak{F}_1$ the field of all automorphic functions with respect to the group $G(\sqrt{M})$ such that their Fourier coefficients belong to the field $\boldsymbol{Q}$. It is known that the field k_M is algebraically closed in $\mathfrak{F}_I$, and the field $\boldsymbol{C}\mathfrak{F}_I$ is the field of all automorphic functions with respect to $\Gamma(I)$ (cf. [**13**, Proposition 1.6]).

Let $f(\tau)$ $(\tau \in \mathfrak{H})$ be an automorphic function with respect to $\Gamma(I)$. If it has no zeros and poles on $\mathfrak{H}$, we call f a *modular unit* with respect to $\Gamma(I)$ and also a *modular unit* on the curve X_I. Later (in Subsection 2.4) we construct modular units contained in the field $\mathfrak{F}_I$.

We denote by $\mathscr{G}_I$ the subgroup of $GL_2(\mathscr{O}/I)$ consisting of all elements α which can be represented by a matrix A $(\in M_2(\mathscr{O}))$ of the form

$$A = \begin{pmatrix} a\sqrt{r} & b\sqrt{r^*} \\ c\sqrt{r^*} & d\sqrt{r} \end{pmatrix}, \tag{2.4}$$

where $a, b, c, d \in \boldsymbol{Z}$, $r \in T$ and $r^* = M/r$. Then it is known that the field $\mathfrak{F}_I$ is a Galois extension of $\mathfrak{F}_1$, and its Galois group is isomorphic to the group $\mathscr{G}_I/\{\pm 1_2\}$ ([**13**, Section 1 (1.15)]). We denote by $\mathscr{G}_I(\pm)$ the group $\mathscr{G}_I/\{\pm 1_2\}$. Then we have

$$\mathrm{Gal}\big(\mathfrak{F}_I/\mathfrak{F}_1\big) \cong \mathscr{G}_I(\pm). \tag{2.5}$$

Let α be an element of $\mathscr{G}_I$ or $\mathscr{G}_I(\pm)$. We denote by $\sigma(\alpha)$ the element of the Galois group $\mathrm{Gal}(\mathfrak{F}_I/\mathfrak{F}_1)$ corresponding to α by (2.5). Let α be represented by the matrix

A in (2.4). Then the element r of T is determined only by α. We call r the *type* of α, and denote it by $t(\alpha)$.

2.3. A summary of properties of Siegel functions.

Here we summarize some properties of Siegel functions, and in the next subsection construct modular units on X_I.

For any element $a = (a_1, a_2)$ of the set $\boldsymbol{Q}^2 - \boldsymbol{Z}^2$, the Siegel function $g_a(\tau)$ ($\tau \in \mathfrak{H}$) is defined in [**7**]. It has the following q-product

$$g_a(\tau) = -q_\tau^{(1/2)B_2(a_1)} e^{2\pi i a_2(a_1-1)/2}(1-q_z)\prod_{k=1}^{\infty}(1-q_\tau^k q_z)\left(1-\frac{q_\tau^k}{q_z}\right), \tag{2.6}$$

where $q_\tau = e^{2\pi i\tau}$, $q_z = e^{2\pi i z}$, $z = a_1\tau + a_2$, and $B_2(X) = X^2 - X + 1/6$ (the second Bernoulli polynomial). If $b = (b_1, b_2) \in \boldsymbol{Z}^2$, then we have

$$g_{a+b}(\tau) = \varepsilon(a,b) g_a(\tau), \tag{2.7}$$

where $\varepsilon(a,b)$ is a root of unity defined by

$$\varepsilon(a,b) = \exp\left[\pi i(b_1b_2 + b_1 + b_2 + a_1b_2 - a_2b_1)\right]. \tag{2.8}$$

If $\alpha \in SL_2(\boldsymbol{Z})$, then we have

$$g_a(\alpha(\tau)) = \psi(\alpha) g_{a\alpha}(\tau), \tag{2.9}$$

where ψ denotes the character of $SL_2(\boldsymbol{Z})$ appearing in the transformation formula of the square of the Dedekind η-function. Explicitly the value of $\psi(\alpha)$ at $\alpha = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right)$ is given by

$$\psi(\alpha) = \begin{cases} (-1)^{(d-1)/2}\exp\left[\dfrac{2\pi i}{12}\{(b-c)d + ac(1-d^2)\}\right] & \text{if } d \text{ is odd,} \\ -i(-1)^{(c-1)/2}\exp\left[\dfrac{2\pi i}{12}\{(a+d)c + bd(1-c^2)\}\right] & \text{if } c \text{ is odd.}\end{cases} \tag{2.10}$$

In particular, we note that $\psi(-1_2) = -1$. (It is known that the kernel of ψ is a congruence subgroup of level 12 with index 12, and coincides with the commutator subgroup of $SL_2(\boldsymbol{Z})$.)

2.4. Modified Siegel functions relative to the ideal $\boldsymbol{I}$.

Let $I=\sqrt{M}\mathscr{O}$ as above. Here we define the modified Siegel functions relative to the ideal I which are suitable for $\Gamma(I)$. In [**18**], for an arbitrary non-zero ideal I $(\neq \mathscr{O})$, the modified Siegel functions relative to the ideal I are defined, and their basic properties are studied. Also in [**16**, Section 1] the case where the ideal I is of the form $I=n\sqrt{m}\mathscr{O}$ is stated.

Let r be an element of T and $r^*=M/r$. Let $A_I'^{(r)}$ be the set of all row vectors u of the form

$$u=\left(\frac{x}{r}\sqrt{r},\frac{y}{r^*}\sqrt{r^*}\right), \tag{2.11}$$

where x and y are rational integers satisfying $u\notin \boldsymbol{Z}\sqrt{r}\times\boldsymbol{Z}\sqrt{r^*}=Z^{(r)}$. We call the element r of T above the *type* of u and denote it by $t(u)$. Put $A_I'=\bigcup_{r\in T}A_I'^{(r)}$ (disjoint). If u is an element of A_I' of type r, and α an element of $G(\sqrt{M})$ of type s $(r,s\in T)$, then the product $u\alpha$ is an element of A_I' of type $r\circ s$.

Let $u=(a_1\sqrt{r},a_2\sqrt{r^*})$ be an element of $\boldsymbol{Q}\sqrt{r}\times\boldsymbol{Q}\sqrt{r^*}-Z^{(r)}$ $(a_1,a_2\in\boldsymbol{Q}$, $r\in T)$, and put $u^\circ=(a_1,a_2)$ $(\in\boldsymbol{Q}^2-\boldsymbol{Z}^2)$. We define the *modified Siegel function* $g_u(\tau)$ $(\tau\in\mathfrak{H})$ by

$$g_u(\tau)=g_{u^\circ}\left(\sqrt{\frac{r}{r^*}}\times\tau\right). \tag{2.12}$$

In particular, if $u\in A_I'$, we say that $g_u(\tau)$ is a modified Siegel function *relative to* the ideal I.

Let $u\in A_I'$ be written as (2.11). Then we have the explicit product

$$\begin{aligned} g_u(\tau)=(-1)\exp\left[\frac{2\pi i}{2}\cdot\frac{y}{r^*}\left(\frac{x}{r}-1\right)\right]&\times t^{(r/2)B_2(x/r)}\\ \times\left(1-\zeta_M^{ry}t^x\right)\prod_{k=1}^{\infty}&\left(1-\zeta_M^{ry}t^{x+rk}\right)\left(1-\zeta_M^{-ry}t^{-x+rk}\right)\end{aligned} \tag{2.13}$$

with $\zeta_M=\exp[2\pi i/M]$ and $t=\exp[2\pi i\tau/\sqrt{M}]$.

For an element $v=(b_1\sqrt{r},b_2\sqrt{r^*})$ of $Z^{(r)}$ $(b_1,b_2\in\boldsymbol{Z})$, write $v^\circ=(b_1,b_2)$ $(\in\boldsymbol{Z}^2)$. For elements $u\in A_I'^{(r)}$ and $v\in Z^{(r)}$, we put

$$\varepsilon(u,v)=\varepsilon(u^\circ,v^\circ). \tag{2.14}$$

Let

$$\alpha = \begin{pmatrix} a\sqrt{s} & b\sqrt{s^*} \\ c\sqrt{s^*} & d\sqrt{s} \end{pmatrix} \tag{2.15}$$

be an element of $G(\sqrt{M})$ of type s $(a, b, c, d \in \boldsymbol{Z},\ s \in T)$. For an element r of T, we put

$$\alpha^{(r)} = \begin{pmatrix} a(r, s) & b(r, s^*) \\ c(r^*, s^*) & d(r^*, s) \end{pmatrix}. \tag{2.16}$$

Then the matrix $\alpha^{(r)}$ belongs to $SL_2(\boldsymbol{Z})$.

Now we have the following transformation formulae ([**16**, Proposition 1.1], [**18**, Proposition 3.5]).

Proposition 2.1. *Let u be an element of A'_I of type r.*

(1) *Let $v \in Z^{(r)}$. Then $g_{u+v}(\tau) = \varepsilon(u, v) g_u(\tau)$.*
(2) *Let $\alpha \in G(\sqrt{M})$. Then $g_u(\alpha(\tau)) = \psi_r(\alpha) g_{u\alpha}(\tau)$, where $\psi_r(\alpha) = \psi(\alpha^{(r)})$.*
(3) *Let $\alpha \in \Gamma(I)$. Then $g_u(\alpha(\tau)) = \varepsilon_u(\alpha)\psi_r(\alpha) g_u(\tau)$, where $\varepsilon_u(\alpha) = \varepsilon(u, v)$ with $v = u\alpha - u$ $(\in Z^{(r)})$.*

As an immediate consequence, we have the following proposition, which states that the modified Siegel functions generate modular units on the curve X_I. (For the proof, see the arguments after [**16**, Proposition 1.1] or the proof of [**18**, Theorem 3.1].)

Proposition 2.2. *Let u be an element of A'_I of type r. Let $[2M, 12]$ be the least common multiple of $2M$ and 12. Then the function $g_u^{[2M,12]}$ depends only on the residue class of u modulo $Z^{(r)}$, and is invariant under the exchange $u \to -u$. Moreover, the function $g_u^{[2M,12]}$ is an automorphic function with respect to $\Gamma(I)$, has no zeros and poles on $\mathfrak{H}$, and its Fourier coefficients belong to the cyclotomic field $k_M = \boldsymbol{Q}(e^{2\pi i/M})$. Hence it is a modular unit contained in the field $\mathfrak{F}_I$.*

2.5. The Galois action on the function $g_u^{[2M,12]}$.

By Proposition 2.2 the function $g_u^{[2M,12]}$ $(u \in A'_I)$ is an element of the function field $\mathfrak{F}_I$. Here we consider the action of the Galois group $\mathrm{Gal}(\mathfrak{F}_I/\mathfrak{F}_1)$ on $g_u^{[2M,12]}$.

For each $r \in T$, put

$$\mathscr{A}_I'^{(r)} = \bigl(A_I'^{(r)}/Z^{(r)}\bigr)/\{\pm 1\} \tag{2.17}$$

and

$$\mathscr{A}_I' = \bigcup_{r\in T} \mathscr{A}_I'^{(r)} \quad \text{(disjoint)}. \tag{2.18}$$

Let u be an element of A_I'. We denote by $[u]$ the class of u in $\mathscr{A}_I'$. By Proposition 2.2 the function $g_u^{[2M,12]}$ depends only on the class $[u]$ of u. Therefore, for any element v of $\mathscr{A}_I'$, we can denote by $g_v^{[2M,12]}$ the function $g_u^{[2M,12]}$ with $v=[u]$. If $v \in \mathscr{A}_I'^{(r)}$, we call r the *type* of v and denote it by $t(v)$.

Let v be an element of $\mathscr{A}_I'$ with $v=[u]$ $(u \in A_I')$. Let α be an element of $\mathscr{G}_I$ or $\mathscr{G}_I(\pm)$, and represented by a matrix A of the form (2.4). Then the product uA belongs to A_I'. We denote by $v\alpha$ the element of $\mathscr{A}_I'$ which is represented by uA. The class $v\alpha$ does not depend on the choice of u and A. This defines the action of $\mathscr{G}_I$ on the set $\mathscr{A}_I'$, and also of $\mathscr{G}_I(\pm)$. If v is of type r and α is of type s, then $v\alpha$ is of type $r\circ s$. Concerning the Galois action on $g_v^{[2M,12]}$ we have the following. (For the proof, see [**13**, (2.5)] or the proof of [**18**, Theorem 3.2].)

Proposition 2.3. *Let $v \in \mathscr{A}_I'$ and $\alpha \in \mathscr{G}_I$. Then we have $\bigl(g_v^{[2M,12]}\bigr)^{\sigma(\alpha)} = g_{v\alpha}^{[2M,12]}$.*

2.6. The Cartan group and the cuspidal prime divisors.

Let C_I be the subgroup of $\mathscr{G}_I$ consisting of all elements α which can be represented by a matrix A $(\in M_2(\mathscr{O}))$ of the form

$$A = \begin{pmatrix} a\sqrt{r} & b\sqrt{r^*} \\ b\sqrt{r^*} & a\sqrt{r} \end{pmatrix} \tag{2.19}$$

with $a, b \in \boldsymbol{Z}$, $r \in T$ and $(ar, br^*, M) = 1$. It is an abelian subgroup of $\mathscr{G}_I$, and called a *Cartan group.*

Let H_I be the subgroup of $\mathscr{G}_I$ consisting of all elements α which can be represented by a matrix B $(\in M_2(\mathscr{O}))$ of the form

$$B = \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \tag{2.20}$$

with $d \in \boldsymbol{Z}$ and $(d, M) = 1$.

We have the following

$$\mathscr{G}_I = H_I C_I \text{ and } H_I \cap C_I = 1. \tag{2.21}$$

Let P_∞ denote the prime divisor of $\mathfrak{F}_I$ defined by the q-expansion. Let P be a prime divisor of $\mathfrak{F}_I$, and ν_P the valuation of P. For any element σ of $\mathrm{Gal}(\mathfrak{F}_I/\mathfrak{F}_1)$, we define the prime divisor P^σ by $\nu_{P^\sigma}(h^\sigma) = \nu_P(h)$ ($h \in \mathfrak{F}_I$), which defines a right action of the group $\mathrm{Gal}(\mathfrak{F}_I/\mathfrak{F}_1)$. We can prove the following (i), (ii), (iii) and (iv) (cf. [**13**, Section 2.1], [**18**, Proposition 4.1]).

(i) The conjugates P_∞^σ are of degree one, hence the prime divisors P_∞^σ can be regarded as prime divisors of the function field $\boldsymbol{C}\mathfrak{F}_I$ and identified with points on the curve X_I.

(ii) If $\alpha \in \mathscr{G}_I$ is an element represented by a matrix $A \in G(\sqrt{M})$, then the prime divisor $P_\infty^{\sigma(\alpha)}$ corresponds to the cusp on X_I represented by $A^{-1}(\infty)$.

(iii) The set of all elements $\alpha \in \mathscr{G}_I$ satisfying $P_\infty^{\sigma(\alpha)} = P_\infty$ coincides with the group $\pm H_I$.

(iv) Let $\mathscr{G}_u(I)$ be the subgroup of $\mathscr{G}_I$ consisting of all elements which can be represented by the matrices A of the form (2.4) satisfying $\det(A) \equiv 1 \pmod{I}$. Then we have $\mathscr{G}_I = \mathscr{G}_u(I)H_I$, and for any element $\alpha \in \mathscr{G}_u(I)$ there exists an element $A \in G(\sqrt{M})$ such that $\alpha = A \pmod{I}$ ([**13**, Proposition 1.1]).

By (2.21) and (iii), every conjugate P_∞^σ can be written as $P_\infty^{\sigma(\alpha)}$ with a unique element α of $C_I(\pm) = C_I/\{\pm 1_2\}$. By (i), (ii) and (iv) any conjugate P_∞^σ can be identified with a cusp on X_I. Conversely it is known that any cusp on X_I can be represented by a point $A^{-1}(\infty)$ with $A \in G(\sqrt{M})$. Thus the group $C_I(\pm)$ and the set of cusps on the curve X_I correspond bijectively by the mapping $\alpha \mapsto P_\infty^{\sigma(\alpha)}$.

We call the conjugates P_∞^σ the *cuspidal prime divisors.*

2.7. The divisor of the function $g_v^{[2M,12]}$.

By Proposition 2.2 the function $g_v^{[2M,12]}$ ($v \in \mathscr{A}_I'$) is an element of the function field $\mathfrak{F}_I$. Here we determine the divisor of $g_v^{[2M,12]}$ as an element of $\mathfrak{F}_I$.

For any $x \in \boldsymbol{R}$ we denote by $\langle x \rangle$ the real number defined by $0 \leqq \langle x \rangle < 1$ and $\langle x \rangle \equiv x \pmod{\boldsymbol{Z}}$. Let $v = [u]$ with $u = (a_1\sqrt{r}, a_2\sqrt{r^*}) \in A_I'^{(r)}$ ($a_1, a_2 \in \boldsymbol{Q}$). Then the number $B_2(\langle a_1 \rangle)$ depends only on v but not on the choice of u because of the equation $B_2(\langle -x \rangle) = B_2(\langle x \rangle)$. Therefore we can denote it by $B_2(\langle v_1^\circ \rangle)$. The following proposition can be proved in the same way as [**13**, Proposition 2.3] or [**14**, Theorem 2.1], and is proved in the case where I is an arbitrary ideal in [**18**, Theorem 4.2]. But for completeness we give the proof.

Proposition 2.4. *Let v be an element of $\mathscr{A}_I'$ with $t(v) = r$. Then the* *divisor of* $g_v^{[2M,12]}$ *as an element of* $\mathfrak{F}_I$ *is given by*

$$\operatorname{div}\bigl(g_v^{[2M,12]}\bigr) = \frac{[2M,12]}{2} \sum_{\alpha \in C_I(\pm)} (r \circ t(\alpha)) B_2\bigl(\langle (v\alpha)_1^\circ \rangle\bigr) P_\infty^{\sigma(\alpha^{-1})}.$$

Proof. Let $v = [u]$ with $u = (a_1\sqrt{r}, a_2\sqrt{r^*}) \in A_I'^{(r)}$ $(a_1, a_2 \in \boldsymbol{Q})$. We can choose the representative u so as to satisfy $0 \leqq a_1 < 1$. Let us write $a_1 = x/r$ with $x \in \boldsymbol{Z}$. Then, in the product (2.13), $x + rk$ and $-x + rk$ are non-negative integers for all $k \in \boldsymbol{Z}$ with $k \geqq 1$. Since the number $\nu_{P_\infty}\bigl(g_v^{[2M,12]}\bigr)$ is equal to the order of $g_v^{[2M,12]}$ with respect to $t = \exp[2\pi i\tau/\sqrt{M}]$, by (2.13), we have

$$\nu_{P_\infty}\bigl(g_v^{[2M,12]}\bigr) = \frac{[2M,12]}{2} r B_2(a_1) = \frac{[2M,12]}{2} r B_2(\langle v_1^\circ \rangle). \tag{2.22}$$

Let α be an element of $C_I(\pm)$. Then $\nu_{P_\infty^{\sigma(\alpha^{-1})}}\bigl(g_v^{[2M,12]}\bigr) = \nu_{P_\infty}\bigl(\bigl(g_v^{[2M,12]}\bigr)^{\sigma(\alpha)}\bigr) = \nu_{P_\infty}\bigl(g_{v\alpha}^{[2M,12]}\bigr)$ (Proposition 2.3). Combining this equation with (2.22) above, we have the desired formula, which completes the proof. □

Let $\mathscr{D}$ be the free abelian group generated by the cuspidal prime divisors of $\mathfrak{F}_I$, and $\mathscr{D}_0$ the subgroup of $\mathscr{D}$ consisting of all elements of degree 0. Let $R = \boldsymbol{Z}[C_I(\pm)]$ be the group ring of $C_I(\pm)$, and R_0 the additive subgroup of R consisting of all elements of degree 0. Let

$$\varphi : \mathscr{D} \cong R \tag{2.23}$$

be the isomorphism defined by the mapping $P_\infty^{\sigma(\alpha)} \mapsto \alpha$. Then we have $\varphi(\mathscr{D}_0) = R_0$. Concerning the product in R we have the following.

Proposition 2.5. *Let* $v \in \mathscr{A}_I'$ *and* $\alpha \in C_I(\pm)$. *Then we have*

$$\alpha\varphi\bigl(\operatorname{div}\bigl(g_v^{[2M,12]}\bigr)\bigr) = \varphi\bigl(\operatorname{div}\bigl(g_{v\alpha}^{[2M,12]}\bigr)\bigr).$$

Proof. Put $\varphi\bigl(\operatorname{div}\bigl(g_v^{[2M,12]}\bigr)\bigr) = \sum_{\beta \in C_I(\pm)} f_v(\beta)\beta$ with $f_v(\beta) \in \boldsymbol{Z}$. Then $f_v(\beta) = \nu_{P_\infty^{\sigma(\beta)}}\bigl(g_v^{[2M,12]}\bigr)$. Multiplying $\varphi\bigl(\operatorname{div}\bigl(g_v^{[2M,12]}\bigr)\bigr)$ by α we have

$$\alpha\varphi\bigl(\operatorname{div}\bigl(g_v^{[2M,12]}\bigr)\bigr) = \sum_{\beta \in C_I(\pm)} f_v(\beta)\alpha\beta = \sum_{\gamma \in C_I(\pm)} f_v(\alpha^{-1}\gamma)\gamma.$$

The coefficient $f_v(\alpha^{-1}\gamma)$ is equal to $\nu_{P_\infty^{\sigma(\alpha^{-1}\gamma)}}\bigl(g_v^{[2M,12]}\bigr) = \nu_{P_\infty^{\sigma(\gamma)}}\bigl(\bigl(g_v^{[2M,12]}\bigr)^{\sigma(\alpha)}\bigr)$. By Proposition 2.3, we have

$$\nu_{P_\infty^{\sigma(\gamma)}}\bigl(\bigl(g_v^{[2M,12]}\bigr)^{\sigma(\alpha)}\bigr) = \nu_{P_\infty^{\sigma(\gamma)}}\bigl(g_{v\alpha}^{[2M,12]}\bigr).$$

Thus we have $f_v(\alpha^{-1}\gamma) = f_{v\alpha}(\gamma)$, which implies $\alpha\varphi\bigl(\mathrm{div}\bigl(g_v^{[2M,12]}\bigr)\bigr) = \varphi\bigl(\mathrm{div}\bigl(g_{v\alpha}^{[2M,12]}\bigr)\bigr)$. Thus the proof is completed. □

2.8. Representatives of $\mathscr{A}'_I$.

Let u be an element of A'_I of type r. It is obvious that $Mu \in Z^{(r)}$ (see (2.11)). Let l be the least natural number such that $lu \in Z^{(r)}$. Then we say that u is of *order* l. Since any element u' of $[u]$ is also of order l, we call l the *order* of the class $[u]$. Let $\mathscr{A}'_I(l)$ (respectively $\mathscr{A}'^{(r)}_I(l)$) be the subset of $\mathscr{A}'_I$ (respectively $\mathscr{A}'^{(r)}_I$) consisting of all elements of order l. Then we have the following decomposition

$$\mathscr{A}'_I = \bigcup_{l\neq 1, \in T} \mathscr{A}'_I(l) \quad \text{(disjoint)}. \tag{2.24}$$

For each l, we define the element $w_l \in A'^{(M)}_I$ by

$$w_l = \left(\frac{1}{l}\sqrt{M}, 0\right). \tag{2.25}$$

Concerning the group action of $C_I(\pm)$ on $\mathscr{A}'_I$ we have the following.

Proposition 2.6. *Let $l \neq 1, \in T$. Then the set $\mathscr{A}'_I(l)$ is an orbit of $C_I(\pm)$, and $\mathscr{A}'_I(l) = [w_l]C_I(\pm)$.*

Proof. Elementary. □

Let $\mathscr{R}^{(r)}_I$ $(r \in T)$ be the subset of $A'^{(r)}_I$ consisting of all elements u of the form (2.11) satisfying one of the following conditions:

(i) $x = 0$, and $0 < y/r^* \leqq 1/2$,
(ii) $0 < x/r \leqq 1/2$, and $0 \leqq y/r^* < 1$.

Put $\mathscr{R}_I = \bigcup_{r\in T} \mathscr{R}^{(r)}_I$. We call the elements of $\mathscr{R}_I$ *reduced*. For each l $(l \neq 1, \in T)$, let $\mathscr{R}^{(r)}_I(l)$ be the subset of $\mathscr{R}^{(r)}_I$ consisting of all elements of order l, and put $\mathscr{R}_I(l) = \bigcup_{r\in T} \mathscr{R}^{(r)}_I(l)$. Then the sets $\mathscr{R}_I$, $\mathscr{R}^{(r)}_I$, $\mathscr{R}_I(l)$ and $\mathscr{R}^{(r)}_I(l)$ are the complete sets of representatives of $\mathscr{A}'_I$, $\mathscr{A}'^{(r)}_I$, $\mathscr{A}'_I(l)$ and $\mathscr{A}'^{(r)}_I(l)$ respectively.

2.9. Square roots of g_u with u of order 2.

Let $l = 2$ (when M is even). Then the set $\mathscr{R}_I^{(r)}(2)$ contains only one element which is $(0, (1/2)\sqrt{r^*})$ or $((1/2)\sqrt{r}, 0)$ according as $2 \nmid r$ or $2 \mid r$. It is known that if u is of order 2 the function $g_u(\tau)$ is a square of a product of (modified) Siegel functions up to a constant. For definiteness, for $u \in \mathscr{R}_I^{(r)}(2)$, we denote by $\sqrt{g_u}(\tau)$ one of the two square roots of $g_u(\tau)$ as follows:

$$\sqrt{g_{(0,(1/2)\sqrt{r^*})}}(\tau) = \sqrt{2}\exp\left[\frac{2\pi i}{8}\right] \cdot t^{r/24} \prod_{k=1}^{\infty}(1 + t^{rk}), \tag{2.26}$$

$$\sqrt{g_{((1/2)\sqrt{r},0)}}(\tau) = \exp\left[-\frac{2\pi i}{4}\right] \cdot t^{-r/48} \prod_{k=1}^{\infty}(1 - t^{rk-r/2}), \tag{2.27}$$

where $t = \exp[2\pi i(\tau/\sqrt{M})]$. (These are the same as [**16**, (2.5), (2.6)].) Then, for example, these functions can be written as follows:

$$\sqrt{g_{(0,(1/2)\sqrt{r^*})}}(\tau) = c \times g_{(0,(1/4)\sqrt{r^*})}(\tau) \times g_{((1/2)\sqrt{r},(1/4)\sqrt{r^*})}(\tau), \tag{2.28}$$

$$\sqrt{g_{((1/2)\sqrt{r},0)}}(\tau) = (-c) \times g_{((1/4)\sqrt{r},0)}(\tau) \times g_{((1/4)\sqrt{r},(1/2)\sqrt{r^*})}(\tau), \tag{2.29}$$

where $c = \exp[2\pi i \cdot 7/16]$.

2.10. Relations between the modified Siegel functions (1).

We define the notation $\hat{g}_u(\tau)$ as follows.

$$\hat{g}_u(\tau) = \begin{cases} g_u(\tau) & \text{if the order of } u \text{ is not 2,} \\ \sqrt{g_u}(\tau) & \text{if } u \in \mathscr{R}_I(2). \end{cases} \tag{2.30}$$

Here, we do not define the notation $\hat{g}_u(\tau)$ for u which is of order 2 but $\notin \mathscr{R}_I(2)$.

Put

$$f_r^{(p)}(\tau) = \prod_{u \in \mathscr{R}_I^{(r)}(p)} \hat{g}_u(\tau). \tag{2.31}$$

Then the function $f_r^{(p)}(\tau)$ can be expressed using the Dedekind η-function $\eta(\tau)$. In fact, Put

$$H(\tau) = \eta\left(\frac{\tau}{\sqrt{M}}\right) = t^{1/24} \prod_{k=1}^{\infty}(1 - t^k) \tag{2.32}$$

with $t = \exp[2\pi i(\tau/\sqrt{M})]$. Then we have

$$f_r^{(p)}(\tau) = c(p,r) \times \frac{H((p \circ r)\tau)}{H(r\tau)}, \tag{2.33}$$

where

$$c(p,r) = \begin{cases} \sqrt{p}\exp\left[2\pi i \cdot \dfrac{p-1}{8}\right] & \text{if } p \nmid r, \\ \exp\left[-2\pi i \cdot \dfrac{p-1}{4}\right] & \text{if } p \mid r \end{cases} \tag{2.34}$$

([**16**, Proposition 2.2]). The following proposition gives relations between the functions $\hat{g}_u(\tau)$ with u reduced and of prime orders.

PROPOSITION 2.7. *Let r be an element of T.*

(1) *Let p be a prime factor of M. Then, we have*

$$f_r^{(p)}(\tau) \times f_{p \circ r}^{(p)}(\tau) = \sqrt{p}\exp\left[-2\pi i \cdot \frac{p-1}{8}\right].$$

(2) *Let p and q be two different prime factors of M. Then we have*

$$\frac{f_r^{(p)}(\tau)}{f_{q \circ r}^{(p)}(\tau)} = \frac{f_r^{(q)}(\tau)}{f_{p \circ r}^{(q)}(\tau)}.$$

PROOF.

(1) By (2.33) we have

$$f_r^{(p)}(\tau) \cdot f_{p \circ r}^{(p)}(\tau) = \frac{c(p,r) \cdot H((p \circ r)\tau)}{H(r\tau)} \cdot \frac{c(p,p \circ r) \cdot H(r\tau)}{H((p \circ r)\tau)} = c(p,r) \cdot c(p, p \circ r),$$

which is equal to $\sqrt{p}\exp[-2\pi i \cdot (p-1)/8]$ by (2.34).

(2) Since $c(p,r) = c(p, q \circ r)$ by (2.34), we have, by (2.33),

$$\frac{f_r^{(p)}(\tau)}{f_{q \circ r}^{(p)}(\tau)} = \frac{H((p \circ r)\tau) \cdot H((q \circ r)\tau)}{H(r\tau) \cdot H((p \circ q \circ r)\tau)},$$

which is symmetrical about p and q. Hence p and q can be exchanged with each other. □

2.11. Relations between the modified Siegel functions (2).

Here we give another type of relations between the functions $\hat{g}_u(\tau)$.

Proposition 2.8. *Let k and l be two elements of T with $(k,l)=1$ and $l \neq 1$. Then we have*

$$\hat{g}_{((1/l)\sqrt{l},0)}(\tau) = (-1)^{N(k,l)} \prod_{x=0}^{N(k,l)} \hat{g}_{((1/(kl)+x/k)\sqrt{kl},0)}(\tau),$$

where $N(k,l) = k-1$ or $(1/2)(k-1)$ according as $l \neq 2$ or $l = 2$.

Remark 2.1. Note that if a notation $\hat{g}_u(\tau)$ with u of order 2 appears in the equation of the proposition, then u is reduced, hence it is well-defined.

Proof. Put $t = \exp[2\pi i(\tau/\sqrt{M})]$ and $u = ((1/(kl)+x/k)\sqrt{kl},0)$. First, we consider the case $l=2$. By (2.27), we have

$$\hat{g}_{((1/l)\sqrt{l},0)}(\tau) = \sqrt{g_{((1/2)\sqrt{2},0)}(\tau)} = \exp\left[-\frac{2\pi i}{4}\right] \cdot t^{-1/24} \prod_{h=1}^{\infty}(1-t^{2h-1}). \quad (2.35)$$

If $0 \leqq x \leqq (1/2)(k-1)-1$, then the order of u is not 2, and if $x = (1/2)(k-1)$, then $u = ((1/2)\sqrt{2k},0)$. Hence, if $0 \leqq x \leqq (1/2)(k-1)-1$, we have

$$\begin{aligned} &\hat{g}_{((1/(kl)+x/k)\sqrt{kl},0)}(\tau) \\ &\quad = g_{((1/(kl)+x/k)\sqrt{kl},0)}(\tau) \\ &\quad = -t^{kB_2(1/(2k)+x/k)}\bigl(1-t^{1+2x}\bigr) \prod_{h=1}^{\infty}\bigl(1-t^{2kh+1+2x}\bigr)\bigl(1-t^{2kh-1-2x}\bigr), \quad (2.36) \end{aligned}$$

and if $x = (1/2)(k-1)$, by (2.27), we have

$$\begin{aligned} \hat{g}_{((1/(kl)+x/k)\sqrt{kl},0)}(\tau) &= \sqrt{g_{((1/2)\sqrt{2k},0)}(\tau)} \\ &= \exp\left[-\frac{2\pi i}{4}\right] \cdot t^{-k/24} \prod_{h=1}^{\infty}\bigl(1-t^{2kh-k}\bigr). \quad (2.37) \end{aligned}$$

By (2.35), (2.36) and (2.37), we can prove the equation of the proposition easily.

Next, we consider the case $l \neq 2$. Then we have

$$\begin{aligned}\hat{g}_{((1/l)\sqrt{l},0)}(\tau) &= g_{((1/l)\sqrt{l},0)}(\tau)\\ &= -t^{(1/2)lB_2(1/l)} \prod_{h=0}^{\infty} \bigl(1 - t^{1+lh}\bigr)\bigl(1 - t^{l-1+lh}\bigr). \end{aligned} \tag{2.38}$$

Since for all x the order of u is not 2, we have

$$\begin{aligned}&\hat{g}_{((1/(kl)+x/k)\sqrt{kl},0)}(\tau)\\ &\quad= g_{((1/(kl)+x/k)\sqrt{kl},0)}(\tau)\\ &\quad= -t^{(1/2)klB_2(1/(kl)+x/k)} \prod_{h=0}^{\infty} \bigl(1 - t^{1+lx+klh}\bigr)\bigl(1 - t^{l-1+(k-1-x)l+klh}\bigr). \end{aligned} \tag{2.39}$$

By (2.38) and (2.39), we can prove the equation of the proposition easily. □

Remark 2.2. Proposition 2.8 is a special case of a general relation concerning the modified Siegel functions, which is a generalization of the distribution relation of the ordinary Siegel functions.

2.12. Relations between the elements θ_l.

Let $\varphi : \mathscr{D} \cong R$ be the isomorphism (2.23). Put $\mathscr{D}_{\boldsymbol{Q}} = \mathscr{D} \otimes \boldsymbol{Q}$ and $R_{\boldsymbol{Q}} = R \otimes \boldsymbol{Q}$. Then we have the isomorphism $\mathscr{D}_{\boldsymbol{Q}} \cong R_{\boldsymbol{Q}}$ extending φ, which we also denote by φ.

Let $f(\tau)$ be a function such that $\{f(\tau)\}^e$ is a modular unit in the function field $\mathfrak{F}_I$ for some integer $e \in \boldsymbol{N}$. Then we define the element $\operatorname{div}(f)$ of $\mathscr{D}_{\boldsymbol{Q}}$ by

$$\operatorname{div}(f) = \frac{1}{e} \operatorname{div}(f^e). \tag{2.40}$$

In particular, let v be any element of $\mathscr{A}_I'(l)$ ($l \neq 1, \in T$), and $v = [u]$ with $u \in \mathscr{R}_I(l)$. We denote by $\operatorname{div}(\hat{g}_v)$ the element $\operatorname{div}(\hat{g}_u)$.

Let $v \in \mathscr{A}_I'$ and $\alpha \in C_I(\pm)$. Then, by Proposition 2.5, we have

$$\alpha\varphi(\operatorname{div}(\hat{g}_v)) = \varphi(\operatorname{div}(\hat{g}_{v\alpha})). \tag{2.41}$$

Let w_l ($l \neq 1, \in T$) be the element (2.25). We denote by θ_l the element of $R_{\boldsymbol{Q}}$ defined by

$$\theta_l = \varphi\bigl(\operatorname{div}(\hat{g}_{[w_l]})\bigr). \tag{2.42}$$

Let $St([w_l])$ be the stabilizer of $[w_l]$:

$$St([w_l]) = \{\alpha \in C_I(\pm) \mid [w_l]\alpha = [w_l]\}. \tag{2.43}$$

If $\alpha \in St([w_l])$, then, by (2.41), we have

$$\alpha\theta_l = \theta_l. \tag{2.44}$$

We denote by $C_I^{(r)}$ (respectively $C_I^{(r)}(\pm)$) the subset of C_I (respectively $C_I(\pm)$) consisting of all elements of type r.

About the group $St([w_l])$ we have the following.

Proposition 2.9. *Let l be an element of T with $l \neq 1$.*

(1) *The stabilizer $St([w_l])$ of $[w_l]$ is the subgroup of $C_I^{(1)}(\pm)$ consisting of all elements α which can be represented by matrices of the form $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ with $a \in \boldsymbol{Z}$ satisfying $a \equiv 1 (\mathrm{mod}\, l)$ and $(a, M) = 1$.*

(2) *If $l \neq 2$, then $St([w_l]) \cong (\boldsymbol{Z}/l^*\boldsymbol{Z})^\times$.*

(3) *If $l = 2$, then $St([w_l]) = C_I^{(1)}(\pm) \cong (\boldsymbol{Z}/M\boldsymbol{Z})^\times / \pm 1$.*

Proof.

(1) and (3) can be proved easily.

(2) Let $\alpha \in St([w_l])$ be represented by a matrix $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ with $a \equiv 1 (\mathrm{mod}\, l)$ and $(a, M) = 1$. Since $l \neq 2$, the class of a in $(\boldsymbol{Z}/M\boldsymbol{Z})^\times$ depends only on α, hence the class of a in $(\boldsymbol{Z}/l^*\boldsymbol{Z})^\times$ is determined by α, which we denote by $\psi(\alpha)$. Then it is easy to see that ψ gives an isomorphism $St([w_l]) \cong (\boldsymbol{Z}/l^*\boldsymbol{Z})^\times$. □

Let us denote by $[r]$ $(r \in T)$ the element of $C_I(\pm)$ which is represented by the matrix

$$\begin{pmatrix} \sqrt{r} & \sqrt{r^*} \\ \sqrt{r^*} & \sqrt{r} \end{pmatrix}. \tag{2.45}$$

The following theorem is a restatement of Proposition 2.7 in the language of divisors, and gives relations between the elements θ_l with l primes.

Theorem 2.1. *In the group ring $R_{\boldsymbol{Q}}$, we have the following relations.*

(1) *Let p be a prime factor of M. Then we have*

$$\Bigg(\sum_{\alpha\in C_I^{(1)}(\pm)}\alpha\Bigg)(1+[p])\theta_p=0.$$

(2) *Let p and q be two different prime factors of M. Then we have*

$$\frac{1}{|St([w_p])|}\Bigg(\sum_{\alpha\in C_I^{(1)}(\pm)}\alpha\Bigg)(1+[pq])\theta_p=\frac{1}{|St([w_q])|}\Bigg(\sum_{\alpha\in C_I^{(1)}(\pm)}\alpha\Bigg)(1+[pq])\theta_q.$$

Proof. Let p be a prime factor of M. For each r ($\in T$), let $R\big(C_I^{(r)}(\pm)/St([w_p])\big)$ be a complete set of representatives $\big(\subset C_I^{(r)}(\pm)\big)$ of the quotient set $C_I^{(r)}(\pm)/St([w_p])$. By Proposition 2.6, the set $\mathscr{A}_I'^{(r)}(p)$ consists of all elements $[w_p]\alpha$ with $\alpha\in R\big(C_I^{(r^*)}(\pm)/St([w_p])\big)$. Note that if $\alpha_1\neq\alpha_2$ $\big(\alpha_i\in R\big(C_I^{(r^*)}(\pm)/St([w_p])\big),\ i=1,2\big)$, then $[w_p]\alpha_1\neq[w_p]\alpha_2$. By (2.31) and (2.41), we have

$$\begin{aligned}\varphi\big(\mathrm{div}(f_r^{(p)})\big)&=\sum_{v\in\mathscr{A}_I'^{(r)}(p)}\varphi(\mathrm{div}(\hat g_v))=\sum_{\alpha}\varphi\big(\mathrm{div}(\hat g_{[w_p]\alpha})\big)\\&=\Bigg(\sum_{\alpha}\alpha\Bigg)\theta_p,\end{aligned}\tag{2.46}$$

where α runs through $R\big(C_I^{(r^*)}(\pm)/St([w_p])\big)$. Let s be any element of T. Since, if α runs through $R\big(C_I^{(r^*)}(\pm)/St([w_p])\big)$, then $\alpha[s]$ runs through a complete set of representatives of $C_I^{((s\circ r)^*)}(\pm)/St([w_p])$, we have by (2.46)

$$\varphi\big(\mathrm{div}\,\big(f_{s\circ r}^{(p)}\big)\big)=\Bigg(\sum_{\alpha}\alpha\Bigg)[s]\theta_p.\tag{2.47}$$

(1) By (2.46), (2.47) and (1) of Proposition 2.7, with $r=M$, we have

$$0=\varphi\big(\mathrm{div}\,\big(f_M^{(p)}\cdot f_{p\circ M}^{(p)}\big)\big)=\Bigg(\sum_{\alpha}\alpha\Bigg)(1+[p])\theta_p,\tag{2.48}$$

where α runs through $R\big(C_I^{(1)}(\pm)/St([w_p])\big)$. Since the right-hand side of (2.48) is equal to

$$\frac{1}{|St([w_p])|}\Bigg(\sum_{\alpha\in C_I^{(1)}(\pm)}\alpha\Bigg)(1+[p])\theta_p, \tag{2.49}$$

(1) is proved.

(2) By (1) of Proposition 2.7, (2.46) and (2.47), with $r=M$, we have

$$\begin{aligned}\varphi\Bigg(\operatorname{div}\bigg(\frac{f_M^{(p)}}{f_{q\circ M}^{(p)}}\bigg)\Bigg) &= \varphi\big(\operatorname{div}\big(f_M^{(p)}\cdot f_{p\circ q\circ M}^{(p)}\big)\big)\\ &= \Big(\sum_{\alpha}\alpha\Big)(1+[pq])\theta_p, \end{aligned}\tag{2.50}$$

where α runs through $R\big(C_I^{(1)}(\pm)/St([w_p])\big)$. The term (2.50) is equal to

$$\frac{1}{|St([w_p])|}\Bigg(\sum_{\alpha\in C_I^{(1)}(\pm)}\alpha\Bigg)(1+[pq])\theta_p. \tag{2.51}$$

By (2) of Proposition 2.7, we can exchange p and q in (2.50), whence the relation of (2) follows. □

Let a be an integer which is prime to M. We denote by $\delta_{[a]}$ the element of $C_I^{(1)}(\pm)$ represented by the matrix $\left(\begin{smallmatrix} a & 0\\ 0 & a\end{smallmatrix}\right)$.

The following theorem is a restatement of Proposition 2.8 in the language of divisors.

THEOREM 2.2. *Let k and l be two elements of T with $(k,l)=1$ and $l\neq 1$.*

(1) *In the group ring $R_{\boldsymbol{Q}}$, we have the following relation*

$$[l^*]^{-1}[(kl)^*]\theta_l=\sum_t\left\{\frac{1}{|St([w_{t^*}])\cap St([w_{lt}])|}\Bigg(\sum_{\alpha\in St([w_{t^*}])}\alpha\Bigg)[s]^{-2}\right\}\theta_{lt},$$

where t runs through all positive divisors of k with $s=k/t$.

(2) *Let t be a positive divisor of k. Let a be an integer satisfying $a\equiv -1\,(\mathrm{mod}\,t)$ and $a\equiv 1\,(\mathrm{mod}\,t^*)$, and put $\delta_t=\delta_{[a]}$. Then we have*

$$St([w_{t^*}])\cap St([w_{lt}])=\begin{cases}1 & \textit{if } l\neq 2,\\ \{1,\delta_t\} & \textit{if } l=2.\end{cases}$$

In particular, if $t = 1$ or $t^* = 2$, the intersection is the trivial group.

(3) *Let t be a positive divisor of k, and put $s = k/t$. If $s \equiv \pm 1 \pmod{l}$, then we have*

$$\Bigl(\sum_{\alpha \in St([w_{t^*}])} \alpha\Bigr)[s]^{-2}\theta_{lt} = \Bigl(\sum_{\alpha \in St([w_{t^*}])} \alpha\Bigr)\theta_{lt}.$$

In particular, if $l = 2$ or 3, then the equation above holds for any t.

Proof. (1) Since the following equations hold in the set $\mathscr{A}_I'$

$$\Bigl[\Bigl(\frac{1}{l}\sqrt{l}, 0\Bigr)\Bigr][l^*] = \Bigl[\Bigl(\frac{1}{l}\sqrt{M}, 0\Bigr)\Bigr],$$
$$\Bigl[\Bigl(\frac{1+lx}{kl}\sqrt{kl}, 0\Bigr)\Bigr][(kl)^*] = \Bigl[\Bigl(\frac{1+lx}{kl}\sqrt{M}, 0\Bigr)\Bigr],$$

we have, by Proposition 2.8,

$$[l^*]^{-1}[(kl)^*]\theta_l = \sum_{x=0}^{N(k,l)} \varphi\bigl(\mathrm{div}(\hat{g}_\upsilon)\bigr), \tag{2.52}$$

where $\upsilon = [(((1+lx)/kl)\sqrt{M}, 0)]$.

Let A be the set of all integers $1 + lx$ with $0 \leqq x \leqq N(k,l)$. Then A is a complete set of representatives of $\boldsymbol{Z}/k\boldsymbol{Z}$ or $(\boldsymbol{Z}/k\boldsymbol{Z})/\pm 1$ according as $l \neq 2$ or $l = 2$. Let t be any positive divisor of k, and put $s = k/t$. Let $A(t)$ be the subset of A consisting of all integers a $(\in A)$ with $(a,k) = s$. Then we have the disjoint union

$$A = \bigcup_t A(t). \tag{2.53}$$

Let $B(t)$ be the set of integers a/s with $a \in A(t)$. Then it is easy to see that $B(t)$ is a complete set of representatives of $(\boldsymbol{Z}/t\boldsymbol{Z})^\times$ or $(\boldsymbol{Z}/t\boldsymbol{Z})^\times/\pm 1$ according as $l \neq 2$ or $l = 2$. By (2.52) and (2.53) we have

$$[l^*]^{-1}[(kl)^*]\theta_l = \sum_t \sum_{b \in B(t)} \varphi\bigl(\mathrm{div}(\hat{g}_\upsilon)\bigr), \tag{2.54}$$

where $\upsilon = [((b/lt)\sqrt{M}, 0)]$.

Let $b \in B(t)$. Since $[s]^2 = \delta_{[s+s^*]}$, we have

$$\left[\left(\frac{b}{lt}\sqrt{M}, 0\right)\right][s]^2 = \left[\left(\frac{b(s+s^*)}{lt}\sqrt{M}, 0\right)\right]. \tag{2.55}$$

Since $(b,t) = 1$ and $(s+s^*, M) = 1$, we have $(b(s+s^*), t) = 1$. Let a be an integer with $(a, M) = 1$ satisfying

$$a \equiv b(s+s^*) \pmod{t}, \tag{2.56}$$

$$a \equiv 1 \pmod{t^*}. \tag{2.57}$$

We have $a \equiv 1 \pmod{l}$ by (2.57) because $l \mid t^*$. Also we have $b(s+s^*) \equiv 1 \pmod{l}$ because $s^* \equiv 0 \pmod{l}$ and $bs \equiv 1 \pmod{l}$ since $bs \in A$. Hence we have

$$a \equiv b(s+s^*) \pmod{l}. \tag{2.58}$$

By (2.56) and (2.58) we have

$$a \equiv b(s+s^*) \pmod{lt}. \tag{2.59}$$

By (2.55) and (2.59) we have

$$\left[\left(\frac{b}{lt}\sqrt{M}, 0\right)\right][s]^2 = \left[\left(\frac{a}{lt}\sqrt{M}, 0\right)\right] = [w_{lt}]\delta_{[a]}. \tag{2.60}$$

By (2.57), the element $\delta_{[a]}$ belongs to $St([w_{t^*}])$. Thus we have shown that for each $b \in B(t)$ there exists an element $\alpha \in St([w_{t^*}])$ such that

$$\left[\left(\frac{b}{lt}\sqrt{M}, 0\right)\right][s]^2 = [w_{lt}]\alpha. \tag{2.61}$$

Let α and β be elements of $St([w_{t^*}])$. It is easy to see that $[w_{lt}]\alpha = [w_{lt}]\beta$ if and only if $\alpha\beta^{-1} \in St([w_{lt}])$. For any $b \in B(t)$, let $\phi(b)$ be the class of α in the factor group of $St([w_{t^*}])$ by $St([w_{t^*}]) \cap St([w_{lt}])$ where α is an element of $St([w_{t^*}])$ satisfying the relation (2.61). Then it is easy to see that ϕ is a bijection between the sets $B(t)$ and $St([w_{t^*}])/(St([w_{t^*}]) \cap St([w_{lt}]))$.

Let $b \in B(t)$ and $v = [((b/lt)\sqrt{M}, 0)]$. Let $\alpha \in St([w_{t^*}])$ be an element which satisfies the relation (2.61). Then we have

$$\varphi\big(\mathrm{div}(\hat{g}_\upsilon)\big) = \alpha[s]^{-2}\theta_{lt}, \tag{2.62}$$

whence

$$\sum_{b\in B(t)} \varphi\big(\mathrm{div}(\hat{g}_\upsilon)\big) = \Big(\sum_{\alpha}\alpha\Big)[s]^{-2}\theta_{lt}, \tag{2.63}$$

where α runs through a complete set of representatives of $St([w_{t^*}])/(St([w_{t^*}]) \cap St([w_{lt}]))$. Since the term on the right-hand side of (2.63) is equal to

$$\frac{1}{|St([w_{t^*}]) \cap St([w_{lt}])|}\Big(\sum_{\alpha\in St([w_{t^*}])}\alpha\Big)[s]^{-2}\theta_{lt}, \tag{2.64}$$

(1) is proved.

(2) Let $\alpha \in St([w_{t^*}]) \cap St([w_{lt}])$. Then there exist two integers a and b such that $\alpha = \delta_{[a]} = \delta_{[b]}$ with $(a, M) = (b, M) = 1$, $a \equiv 1 \pmod{t^*}$, and $b \equiv 1 \pmod{lt}$. Since $\delta_{[a]} = \delta_{[b]}$, we have $a \equiv \pm b \pmod{M}$. Assume that $a \equiv b \pmod{M}$. Since $a \equiv 1 \pmod{t^*}$ and $a \equiv b \equiv 1 \pmod{t}$, we have $a \equiv 1 \pmod{M}$, which gives $\alpha = 1$. Next, assume that $a \equiv -b \pmod{M}$. Since $l \mid t^*$, we have $1 \equiv a \equiv -b \equiv -1 \pmod{l}$, whence $2 \equiv 0 \pmod{l}$, which implies $l = 2$. Thus, if $l \neq 2$, the intersection contains only the unity. If $l = 2$, we have $a \equiv -b \equiv -1 \pmod{t}$ and $a \equiv 1 \pmod{t^*}$, hence the unique possible element is $\alpha = \delta_t$. In fact, if $l = 2$, it is easy to see that the element δ_t is contained in both $St([w_{t^*}])$ and $St([w_{lt}])$. This proves the equation of (2). If $t = 1$ or $t^* = 2$, then $\delta_t = 1$, which proves (2).

(3) If $s \equiv \pm 1 \pmod{l}$, then we have $s + s^* \equiv \pm 1 \pmod{l}$ because $l \mid s^*$. If $s \equiv 1 \pmod{l}$ (respectively $s \equiv -1 \pmod{l}$), let a be an integer with $(a, M) = 1$, $a \equiv 1 \pmod{t^*}$ and $a \equiv s+s^* \pmod{t}$ (respectively $a \equiv -(s+s^*) \pmod{t}$), and b be an integer with $(b, M) = 1$, $b \equiv 1 \pmod{lt}$ and $b \equiv s + s^* \pmod{(t^*/l)}$ (respectively $b \equiv -(s + s^*) \pmod{(t^*/l)}$). Then $\delta_{[a]} \in St([w_{t^*}])$ and $\delta_{[b]} \in St([w_{lt}])$. It is easy to see that $ab \equiv s + s^* \pmod{M}$ or $-(s + s^*) \pmod{M}$ according as $s \equiv 1 \pmod{l}$ or $-1 \pmod{l}$ respectively. Since $[s]^2 = \delta_{[s+s^*]}$, we have $[s]^2 = \delta_{[ab]} = \delta_{[a]}\delta_{[b]} \in St([w_{t^*}])St([w_{lt}])$. This proves (3). □

Corollary 2.1. *Assume that M is even with $M \neq 2$ and l is an odd factor of M with $l \neq 1$. Then we have*

$$\theta_{2l} = \big([l^*]^{-1}[(2l)^*] - [2]^{-2}\big)\theta_l.$$

Proof. In the theorem, put $k = 2$. □

Corollary 2.2. *Assume that $M = p_1 p_2$ with p_1 and p_2 different primes.*

(1) *We have the following relation*

$$\Bigl(\sum_{\alpha \in St([w_{p_1}])} \alpha\Bigr)\theta_M = \bigl([p_2]^{-1} - [p_2]^{-2}\bigr)\theta_{p_1}.$$

(2) *In particular, if $p_1 = 2$, then we have*

$$\Bigl(\sum_{\alpha \in C^{(1)}(\pm)} \alpha\Bigr)\theta_M = \bigl([p_2]^{-1} - 1\bigr)\theta_2.$$

(3) *In particular, if $p_2 = 2$, then we have*

$$\theta_M = \bigl([2]^{-1} - [2]^{-2}\bigr)\theta_{p_1}.$$

Proof. In the theorem, put $l = p_1$ and $k = p_2$. □

Remark 2.3. Let $\mathscr{S}$ be the group of all Siegel units in the field $\mathfrak{F}_I$, where we say that a modular unit in $\mathfrak{F}_I$ is a Siegel unit if it can be expressed as a product of the modified Siegel functions $\hat{g}_u(\tau)$ with $u \in \mathscr{R}_I$ up to a constant. Let $\operatorname{div}(\mathscr{S})$ denote the group of principal divisors of all Siegel units in the field $\mathfrak{F}_I$. Let φ be the isomorphism (2.23). Then $\varphi(\operatorname{div}(\mathscr{S}))$ is an ideal of the group ring R, and generated by the elements θ_l with $l \neq 1, \in T$. If M is a prime, then the ideal $\varphi(\operatorname{div}(\mathscr{S}))$ is generated by only one element θ_M. But, if M is composite, except the case where $M = 2p$ with p a prime $\neq 2$, the ideal $\varphi(\operatorname{div}(\mathscr{S}))$ has the generator set $\{\theta_l\}$ consisting of more than two elements, and the relations between the elements θ_l are complicated. On the contrary, in the case where $M = 2p$ with p a prime $\neq 2$, the ideal $\varphi(\operatorname{div}(\mathscr{S}))$ is generated by two elements θ_2 and θ_p by the relation (3) of Corollary 2.2. This is the reason why we confine our study to the case $M = 2p$ in the later sections.

3. The fullness of the Siegel units.

Henceforth we consider the modular curve $X_1(2p)$. We use the notation and the results in the previous section under the assumption that

$$M = 2p, \tag{3.1}$$

where p is a prime with $p \neq 2$.

In this section, we prove that the group $\mathscr{F}$ of the modular units in $\mathfrak{F}_I$ has the maximal possible rank $2p-3$, and that any function in $\mathscr{F}$ can be expressed as a product of the modified Siegel functions up to a constant. In later sections we shall assume that $p \neq 3$.

3.1. The cuspidal divisor class group.

It is easy to see that the number of the elements of $C_I(\pm)$ is equal to $2(p-1)$. Hence the number of the cusps on the curve X_I (or $X_1(2p)$) is also equal to $2(p-1)$.

Let $\mathscr{D}$ and $\mathscr{D}_0$ be as before. Let $\mathscr{F}$ or $\mathscr{F}_{\boldsymbol{C}}$ be the group of all modular units in $\mathfrak{F}_I$ or $\boldsymbol{C}\mathfrak{F}_I$ respectively. Later (in Corollary 3.1) we shall see that $\mathscr{F}_{\boldsymbol{C}} = \boldsymbol{C}^\times \mathscr{F}$ and the divisor group $\operatorname{div}(\mathscr{F})$ can be identified with the divisor group $\operatorname{div}(\mathscr{F}_{\boldsymbol{C}})$. Therefore we call the factor group

$$\mathscr{C} = \mathscr{D}_0/\operatorname{div}(\mathscr{F}) \tag{3.2}$$

the *cuspidal divisor class group* on the curve X_I and the order of $\mathscr{C}$ the *cuspidal class number* of X_I or of $X_1(2p)$.

3.2. Divisors of modified Siegel functions.

The following proposition gives the explicit representations of θ_l.

PROPOSITION 3.1. *For each $l = 2$, p, $2p$, the element θ_l is given as follows. In each summation, the element α runs through the group $C_I(\pm)$ with the described type.*

(1) *Let $l = 2$. Then we have*

$$\theta_2 = \frac{1}{24}\Bigg\{-\sum_{t(\alpha)=1} p\cdot\alpha^{-1} + \sum_{t(\alpha)=2} p\cdot\alpha^{-1} - \sum_{t(\alpha)=p} \alpha^{-1} + \sum_{t(\alpha)=2p} \alpha^{-1}\Bigg\}.$$

(2) *Let $l = p$. If $t(\alpha) = 1$ or 2, we assume that α is represented by a matrix $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} a\sqrt{2} & \sqrt{p} \\ \sqrt{p} & a\sqrt{2} \end{smallmatrix}\right)$ ($a \in \boldsymbol{Z}$) respectively. Then we have*

$$\begin{aligned}\theta_p = &\sum_{t(\alpha)=1} pB_2\left(\left\langle\frac{a}{p}\right\rangle\right)\cdot\alpha^{-1} + \sum_{t(\alpha)=2} \frac{p}{2}B_2\left(\left\langle\frac{2a}{p}\right\rangle\right)\cdot\alpha^{-1} \\ &+ \frac{1}{6}\sum_{t(\alpha)=p} \alpha^{-1} + \frac{1}{12}\sum_{t(\alpha)=2p} \alpha^{-1}.\end{aligned}$$

(3) *Let $l = 2p$. If $t(\alpha) = 1$ or 2, we assume that α is represented by a matrix*

$\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ *or* $\left(\begin{smallmatrix} a\sqrt{2} & \sqrt{p} \\ \sqrt{p} & a\sqrt{2} \end{smallmatrix}\right)$ $(a \in \boldsymbol{Z})$ *respectively. Then we have*

$$\theta_{2p} = \sum_{t(\alpha)=1} pB_2\left(\left\langle\frac{a}{2p}\right\rangle\right) \cdot \alpha^{-1} + \sum_{t(\alpha)=2} \frac{p}{2}B_2\left(\left\langle\frac{a}{p}\right\rangle\right) \cdot \alpha^{-1}$$
$$- \frac{1}{12}\sum_{t(\alpha)=p} \alpha^{-1} + \frac{1}{12}\sum_{t(\alpha)=2p} \alpha^{-1}.$$

Proof. These follow from Proposition 2.4. □

The following proposition gives relations concerning the elements θ_2 and θ_p.

Proposition 3.2. *Concerning the elements θ_2 and θ_p, we have the following relations. In the relations in* (2) *and* (3), *the element α runs through the group $C_I(\pm)$ with the described type.*

(1) *For θ_2 we have*

$$(1 + \beta_2)\theta_2 = 0,$$

where β_2 denotes any element of $C_I(\pm)$ of type 2.

(2) *For θ_p we have*

$$\Bigl(\sum_{t(\alpha)=1} \alpha + \sum_{t(\alpha)=p} \alpha\Bigr)\theta_p = 0.$$

(3) *For θ_2 and θ_p we have*

$$\Bigl(\sum_{t(\alpha)=1} \alpha + \sum_{t(\alpha)=2p} \alpha\Bigr)\theta_p = (1 + \beta_{2p})\theta_2,$$

where β_{2p} denotes any element of $C_I(\pm)$ of type $2p$.

Proof.

(1) By (1) of Theorem 2.1 we have $\bigl(\sum_{\alpha \in C_I^{(1)}(\pm)} \alpha\bigr)(1 + [2])\theta_2 = 0$. Since $\alpha\theta_2 = \theta_2$ for any $\alpha \in C_I^{(1)}(\pm)$ by (3) of Proposition 2.9, we have $\bigl(\sum_{\alpha \in C_I^{(1)}(\pm)} \alpha\bigr)\theta_2 = \bigl|C_I^{(1)}(\pm)\bigr|\theta_2$ and $\bigl(\sum_{\alpha \in C_I^{(1)}(\pm)} \alpha\bigr)[2]\theta_2 = \bigl|C_I^{(1)}(\pm)\bigr|\beta_2\theta_2$ with β_2 any element of $C_I^{(2)}(\pm)$. Hence we have $\bigl|C_I^{(1)}(\pm)\bigr|(1 + \beta_2)\theta_2 = 0$. This proves (1).

(2) By (1) of Theorem 2.1 we have $\big(\sum_{\alpha\in C_I^{(1)}(\pm)}\alpha\big)(1+[p])\theta_p = 0$. Since $\big(\sum_{\alpha\in C_I^{(1)}(\pm)}\alpha\big)[p]=\sum_{\alpha\in C_I^{(p)}(\pm)}\alpha$, we have the relation of (2).

(3) By (2) of Theorem 2.1 we have

$$\frac{1}{|St([w_p])|}\Bigg(\sum_{\alpha\in C_I^{(1)}(\pm)}\alpha\Bigg)(1+[2p])\theta_p = \frac{1}{|St([w_2])|}\Bigg(\sum_{\alpha\in C_I^{(1)}(\pm)}\alpha\Bigg)(1+[2p])\theta_2.$$

Since $|St([w_p])|=1$ by (2) of Proposition 2.9, the left-hand side of the equation above is equal to $\big(\sum_{t(\alpha)=1}\alpha+\sum_{t(\alpha)=2p}\alpha\big)\theta_p$. Also since $St\big([w_2]\big)=C_I^{(1)}(\pm)$ by (3) of Proposition 2.9, the right-hand side of the equation above is equal to $(1+\beta_{2p})\theta_2$. This proves (3). □

The following proposition gives relations between θ_{2p} and θ_l with $l=2$, p.

PROPOSITION 3.3. *Concerning the elements θ_{2p} and θ_l with $l=2$, p, we have the following relations.*

(1) *For θ_2 we have*

$$\Bigg(\sum_{t(\alpha)=1}\alpha\Bigg)\theta_{2p}=\big([p]^{-1}-1\big)\theta_2,$$

where α runs through the group $C_I(\pm)$ with $t(\alpha)=1$.

(2) *For θ_p we have*

$$\theta_{2p}=\big([2]^{-1}-[2]^{-2}\big)\theta_p.$$

PROOF. These are the same as (2) and (3) of Corollary 2.2. □

3.3. Relations between the modified Siegel functions.

The following proposition gives relations between the functions $\hat{g}_u(\tau)$ with $u\in\mathscr{R}_I$.

PROPOSITION 3.4.

(1) *Let u be any element of $\mathscr{R}_I(2p)$. Then the function $\hat{g}_u(\tau)$ can be expressed as a product of the functions $\hat{g}_{u'}(\tau)$ with $u'\in\mathscr{R}_I(p)$ up to a constant.*

(2) *The products $\prod_{u\in\mathscr{R}_I^{(1)}(p)\cup\mathscr{R}_I^{(p)}(p)}\hat{g}_u(\tau)$ and $\prod_{u\in\mathscr{R}_I^{(2)}(p)\cup\mathscr{R}_I^{(2p)}(p)}\hat{g}_u(\tau)$ are constants.*

(3) *The products $\prod_{u\in\mathscr{R}_I^{(1)}(2)\cup\mathscr{R}_I^{(2)}(2)}\hat{g}_u(\tau)$ and $\prod_{u\in\mathscr{R}_I^{(p)}(2)\cup\mathscr{R}_I^{(2p)}(2)}\hat{g}_u(\tau)$ are con-*

stants.

(4) *The products* $\prod_{u\in\mathscr{R}_I^{(1)}(2)\cup\mathscr{R}_I^{(2p)}(2)}\hat{g}_u(\tau)$ *and* $\prod_{u\in\mathscr{R}_I^{(2)}(2)\cup\mathscr{R}_I^{(p)}(2)}\hat{g}_u(\tau)$ *can be expressed as products of the functions* $\hat{g}_{u'}(\tau)$ *with* $u'\in\mathscr{R}_I(p)$ *up to constants.*

Proof. These statements follow from the relations between the elements θ_l, the equation (2.41) and Proposition 2.6.

(1) This follows from (2) of Proposition 3.3.

(2) Multiplying the relation of (2) of Proposition 3.2 by an element of $C_I(\pm)$ of type 2, we have $\big(\sum_{t(\alpha)=2}\alpha+\sum_{t(\alpha)=2p}\alpha\big)\theta_p=0$. The statement of (2) follows from these relations.

(3) Multiplying the relation of (1) of Proposition 3.2 by an element of $C_I(\pm)$ of type p, we have $\beta_p\theta_2+\beta_{2p}\theta_2=0$, where β_p (respectively β_{2p}) denotes an element of $C_I(\pm)$ of type p (respectively $2p$). The statement of (3) follows from these relations.

(4) Multiplying the relation of (3) of Proposition 3.2 by an element of $C_I(\pm)$ of type 2, we have $\big(\sum_{t(\alpha)=2}\alpha+\sum_{t(\alpha)=p}\alpha\big)\theta_p=\beta_2\theta_2+\beta_p\theta_2$, where β_2 (respectively β_p) denotes an element of $C_I(\pm)$ of type 2 (respectively p). The statement of (4) follows from these relations. □

3.4. A generating set of Siegel units.

Let $\mathscr{S}$ be the group of all Siegel units in the field $\mathfrak{F}_I$, where we say that a modular unit in $\mathfrak{F}_I$ is a *Siegel unit* if it can be expressed as a product of the modified Siegel functions $\hat{g}_u(\tau)$ with $u\in\mathscr{R}_I$ up to a constant.

We define the subsets $\mathscr{R}_I^\circ(p)$ and $\mathscr{R}_I^\circ$ of $\mathscr{R}_I$ by

$$\mathscr{R}_I^\circ(p)=\Big(\bigcup_{i=1,p}\mathscr{R}_I^{(i)}(p)-\{u_{(1)}\}\Big)\cup\Big(\bigcup_{i=2,2p}\mathscr{R}_I^{(i)}(p)-\{u_{(2)}\}\Big)\tag{3.3}$$

$$\mathscr{R}_I^\circ=\mathscr{R}_I^\circ(p)\cup\{w_2\}\tag{3.4}$$

where $u_{(1)}$ (respectively $u_{(2)}$) is an arbitrarily chosen element of $\bigcup_{i=1,p}\mathscr{R}_I^{(i)}(p)$ (respectively $\bigcup_{i=2,2p}\mathscr{R}_I^{(i)}(p)$), and w_2 is the element defined by (2.25). We note that $\mathscr{R}_I^{(2p)}(2)=\{w_2\}$.

Proposition 3.5. *Any function g in $\mathscr{S}$ can be written as $g=c\cdot(i\hat{g}_{w_2})^{m(w_2)}\prod_{u\in\mathscr{R}_I^\circ(p)}(g_u)^{m(u)}$ with $c\in k_M^\times$ and $m(u)\in\boldsymbol{Z}$ $(u\in\mathscr{R}_I^\circ)$.*

Proof. Let g be any function in $\mathscr{S}$. Then g is a product of the functions $\hat{g}_u$ with $u\in\mathscr{R}_I$ up to a constant. We can remove the functions $\hat{g}_u$ with $u\in\mathscr{R}_I(2p)$ from the expression of g by (1) of Proposition 3.4. Also we can remove the functions

$\hat{g}_u$ with $u \in \mathscr{R}_I^{(1)}(2) \cup \mathscr{R}_I^{(p)}(2)$ by (3) of Proposition 3.4, and the function $\hat{g}_u$ with $u \in \mathscr{R}_I^{(2)}(2)$ by the combination of (3) and (4) of Proposition 3.4. (Note that each set $\mathscr{R}_I^{(r)}(2)$ $(r \in T)$ contains only one element.) Thus g can be expressed as a product of $\hat{g}_u$ with $u \in \mathscr{R}_I(p) \cup \mathscr{R}_I^{(2p)}(2)$ up to a constant. Let $u_{(1)}$ (respectively $u_{(2)}$) be the element of $\mathscr{R}_I^{(1)}(p) \cup \mathscr{R}_I^{(p)}(p)$ (respectively $\mathscr{R}_I^{(2)}(p) \cup \mathscr{R}_I^{(2p)}(p)$) in (3.3). Then we can remove the functions $\hat{g}_{u_{(1)}}$ and $\hat{g}_{u_{(2)}}$ from the expression of g by (2) of Proposition 3.4. Thus g can be written as a product of the functions $\hat{g}_u$ with $u \in \mathscr{R}_I^{\circ}(p) \cup \mathscr{R}_I^{(2p)}(2)$ and a constant. Let $u \in \mathscr{R}_I^{\circ}(p)$. Then, by (2.13), the Fourier coefficients of $\hat{g}_u = g_u$ belong to k_M. Let $u \in \mathscr{R}_I^{(2p)}(2)$. Since $\mathscr{R}_I^{(2p)}(2) = \{w_2\}$, we have $\hat{g}_u = \hat{g}_{w_2}$. By the definition (2.27) the Fourier coefficients of the product $i \cdot \hat{g}_{w_2}$ belong to k_M. This proves the proposition. □

3.5. The fullness of the Siegel units.

Here we prove that the functions $\hat{g}_u$ with $u \in \mathscr{R}_I^{\circ}$ are independent, and that $\mathscr{S}$ coincides with the group $\mathscr{F}$ of all modular units in $\mathfrak{F}_I$.

Let $\mathfrak{F}^{(M)}$ be the function field defined in [**13**, Section 1.5]. It is the field of all automorphic functions with respect to the congruence subgroups of $G(\sqrt{M})$ such that their Fourier coefficients belong to the cyclotomic fields. Then the field $\boldsymbol{C}\mathfrak{F}^{(M)}$ coincides with the field of all automorphic functions with respect to the congruence subgroups of $G(\sqrt{M})$.

Let u be any element of $\mathscr{R}_I$. Let α be any element of $\mathscr{G}_I$ or $\mathscr{G}_I(\pm)$. Since the set $\mathscr{R}_I$ is a complete set of representatives of $\mathscr{A}_I'$, there exists a uniquely determined element $u' \in \mathscr{R}_I$ such that $[u'] = [u]\alpha$, which we denote by $u \circ \alpha$:

$$[u \circ \alpha] = [u]\alpha. \tag{3.5}$$

It is obvious that if $u \in \mathscr{R}_I^{(r)}(l)$ and $t(\alpha) = s$, then $u \circ \alpha \in \mathscr{R}_I^{(r \circ s)}(l)$.

Since each set $\mathscr{R}_I^{(r)}(2)$ $(r \in T)$ contains only one element, we denote the unique element of $\mathscr{R}_I^{(r)}(2)$ by $u^{(r)}(2)$.

Lemma 3.1. *Let l be a prime, and let $m : \mathscr{R}_I(2) \cup \mathscr{R}_I(p) \to \boldsymbol{Z}$ be a mapping. Assume that there exists a function $g \in \boldsymbol{C}\mathfrak{F}^{(M)}$ such that*

$$\prod_{u \in \mathscr{R}_I(2) \cup \mathscr{R}_I(p)} (\hat{g}_u)^{m(u)} = g^l.$$

Then we have the following.

(1) *Let α be any element of $\mathscr{G}_I$, and let u be any element of $\mathscr{R}_I^{(1)}(p)$. Then*

$$\begin{aligned}&- m\big(u^{(1)}(2)\circ\alpha\big) + m\big(u^{(2)}(2)\circ\alpha\big) + m\left(\left(\frac{1}{p}\sqrt{p}, 0\right)\circ\alpha\right)\\ &\quad\equiv m(u\circ\alpha)\pmod{l}.\end{aligned}$$

(2) *Let u_1 and u_2 be any elements of $\mathscr{R}_I^{(r)}(p)$ $(r\in T)$. Then $m(u_1)\equiv m(u_2)\pmod{l}$.*

Proof. The statement (2) follows immediately from (1) if we take as α any element of type r. We prove (1). The relation of the lemma implies that g belongs to the field $\mathfrak{F}^{(M)}$. Let G_{A+} and U be the groups defined in [**13**, p. 352], and $\sigma: G_{A+}\to \mathrm{Aut}(\mathfrak{F}^{(M)})$ be the homomorphism defined in [**13**, p. 355]. Let $\beta=\alpha^{-1}$, and β_1 an element of U such that $\beta\equiv\beta_1\pmod{I}$ (cf. [**13**, Proposition 1.4]). Then we have $\hat{g}_u^{\sigma(\beta_1)} = (\text{a constant})\hat{g}_{u\circ\beta}$ by Proposition 2.3. Applying the element $\sigma(\beta_1)$ to the equation of the lemma, we have $\prod_{u\in\mathscr{R}_I(2)\cup\mathscr{R}_I(p)}(\hat{g}_{u\circ\beta})^{m(u)} = g_1^l$ where $g_1 = (\text{a constant})g^{\sigma(\beta_1)}$. Let m_1 be the mapping from $\mathscr{R}_I(2)\cup\mathscr{R}_I(p)$ to $\boldsymbol{Z}$ defined by $m_1(u) = m(u\circ\alpha)$. If u runs through $\mathscr{R}_I(2)\cup\mathscr{R}_I(p)$, then so does $u\circ\beta$. We have, therefore, $\prod_{u\in\mathscr{R}_I(2)\cup\mathscr{R}_I(p)}(\hat{g}_u)^{m_1(u)} = g_1^l$. Let f be a non-zero element of $\boldsymbol{C}\mathfrak{F}^{(M)}$ with $\sum_k a_k q_N^k$ its Fourier expansion where $q_N = \exp[2\pi i(\tau/(N\sqrt{M}))]$ $(N\in\boldsymbol{N})$. Let $a_h q_N^h$ be the lowest term. Then the power series $f^* = f/(a_h q_N^h)$ is called the *reduced form* of f (cf. [**7**, p. 88]). Let $\hat{g}_u^*$ and g_1^* be the reduced forms of $\hat{g}_u$ and g_1 respectively. Then we have

$$\prod_{u\in\mathscr{R}_I(2)\cup\mathscr{R}_I(p)} \big(\hat{g}_u^*\big)^{m_1(u)} = \big(g_1^*\big)^l. \tag{3.6}$$

By the q-products (2.13), (2.26) and (2.27), we see that each $\hat{g}_u^*$ is a power series $1+a_1t+\cdots$ in $t=\exp[2\pi i(\tau/\sqrt{M})]$ with coefficients in the ring $\mathfrak{o}_M$ of the algebraic integers in the field k_M. By (3.6), g_1^* is also a power series $1+b_1t+\cdots$ in t with coefficients in the field k_M. By a consequence of a theorem of Shimura [**7**, Lemma 3.1 in Chapter 4], the coefficients of g_1^* have bounded denominators. Thus, by (3.6) and the Gauss lemma for power series with bounded denominators, we see that the power series g_1^* also has coefficients in the integer ring $\mathfrak{o}_M$. Let a_1 be the coefficient of t in the power series $\hat{g}_u^*$. If $u\in\mathscr{R}_I^{(r)}(2)$, then we have

$$a_1 = \begin{cases} 1 & \text{if } r=1, \text{ i.e. } u=u^{(1)}(2)=(0,(1/2)\sqrt{2p}),\\ -1 & \text{if } r=2, \text{ i.e. } u=u^{(2)}(2)=((1/2)\sqrt{2},0),\\ 0 & \text{if } r=p \text{ or } 2p,\end{cases} \tag{3.7}$$

by (2.26) and (2.27). If $u \in R_I^{(r)}(p)$, then we have

$$a_1 = \begin{cases} -\bigl(\zeta_p^b + \zeta_p^{-b}\bigr) & \text{if } r = 1 \text{ and } u = (0, (b/p)\sqrt{2p}) \ (1 \leqq b \leqq (p-1)/2), \\ -1 & \text{if } r = p \text{ and } u = ((1/p)\sqrt{p}, 0), \\ 0 & \text{otherwise}, \end{cases} \tag{3.8}$$

by (2.13), where $\zeta_p = \exp[2\pi i/p]$. Let c_1 be the coefficient of t in the power series expansion of the left-hand side of (3.6). Then we have, by (3.7) and (3.8),

$$\begin{aligned} c_1 = m_1\bigl(u^{(1)}(2)\bigr) - m_1\bigl(u^{(2)}(2)\bigr) - m_1\Bigl(\Bigl(\frac{1}{p}\sqrt{p}, 0\Bigr)\Bigr) \\ - \sum_{b=1}^{(p-1)/2} \bigl(\zeta_p^b + \zeta_p^{-b}\bigr) m_1\Bigl(\Bigl(0, \frac{b}{p}\sqrt{2p}\Bigr)\Bigr). \end{aligned} \tag{3.9}$$

Since c_1 is also the coefficient of t in the power series expansion of $(g_1^*)^l$, and the coefficients of the power series g_1^* are integers, it must be congruent to 0 modulo l. This implies that, by [**7**, Lemma 2.3 in Chapter 4], the following congruences hold

$$\begin{aligned} m_1\bigl(u^{(1)}(2)\bigr) - m_1\bigl(u^{(2)}(2)\bigr) - m_1\Bigl(\Bigl(\frac{1}{p}\sqrt{p}, 0\Bigr)\Bigr) \\ \equiv -m_1\Bigl(\Bigl(0, \frac{b}{p}\sqrt{2p}\Bigr)\Bigr) \pmod{l} \end{aligned} \tag{3.10}$$

for all b $(1 \leqq b \leqq (p-1)/2)$. Since any element of $\mathscr{R}_I^{(1)}(p)$ can be written as $(0, (b/p)\sqrt{2p})$, this completes the proof. □

Lemma 3.2. *Let l be a prime, and let $m : \mathscr{R}_I^\circ \to \boldsymbol{Z}$ be a mapping. Assume that there exists a function $g \in \boldsymbol{C}\mathfrak{F}^{(M)}$ such that*

$$\prod_{u \in \mathscr{R}_I^\circ} (\hat{g}_u)^{m(u)} = g^l.$$

Then $m(u) \equiv 0 \pmod{l}$ for all $u \in \mathscr{R}_I^\circ$.

Proof. We extend the domain of the mapping m from $\mathscr{R}_I^\circ$ to $\mathscr{R}_I(2) \cup \mathscr{R}_I(p)$ by setting $m(u) = 0$ for any $u \in \mathscr{R}_I(2) \cup \mathscr{R}_I(p) - \mathscr{R}_I^\circ$. Since $m(u^{(1)}(2)) =$

$m(u^{(2)}(2))=0$, we have $m(((1/p)\sqrt{p},0))\equiv m(u)\,(\mathrm{mod}\,l)$ for all $u\in\mathscr{R}_I^{(1)}(p)$ by (1) of Lemma 3.1 with $\alpha=1$. By this and (2) of Lemma 3.1, we have $m(u_1)\equiv m(u_2)\,(\mathrm{mod}\,l)$ for any $u_1,u_2\in\mathscr{R}_I^{(1)}(p)\cup\mathscr{R}_I^{(p)}(p)$. By the definition (3.3) of $\mathscr{R}_I^\circ$, there exists an element $u_{(1)}$ of $\mathscr{R}_I^{(1)}(p)\cup\mathscr{R}_I^{(p)}(p)$ which is not contained in $\mathscr{R}_I^\circ$. Then $m(u_{(1)})=0$, hence we have

$$m(u)\equiv 0\,(\mathrm{mod}\,l)\text{ for all }u\in\mathscr{R}_I^{(1)}(p)\cup\mathscr{R}_I^{(p)}(p). \tag{3.11}$$

Next, in (1) of Lemma 3.1, we assume that α is an element of type 2. Then $u^{(1)}(2)\circ\alpha=u^{(2)}(2)$ and $u^{(2)}(2)\circ\alpha=u^{(1)}(2)$. Since $m(u^{(1)}(2))=m(u^{(2)}(2))=0$, we have $m(((1/p)\sqrt{p},0)\circ\alpha)\equiv m(u)\,(\mathrm{mod}\,l)$ for all $u\in\mathscr{R}_I^{(2)}(p)$. By this and (2) of Lemma 3.1, we have $m(u_1)\equiv m(u_2)\,(\mathrm{mod}\,l)$ for any $u_1,u_2\in\mathscr{R}_I^{(2)}(p)\cup\mathscr{R}_I^{(2p)}(p)$. Again by the definition (3.3) of $\mathscr{R}_I^\circ$, there exists an element $u_{(2)}$ of $\mathscr{R}_I^{(2)}(p)\cup\mathscr{R}_I^{(2p)}(p)$ which does not contained in $\mathscr{R}_I^\circ$. Since $m(u_{(2)})=0$, we have

$$m(u)\equiv 0\,(\mathrm{mod}\,l)\text{ for all }u\in\mathscr{R}_I^{(2)}(p)\cup\mathscr{R}_I^{(2p)}(p). \tag{3.12}$$

Last, in (1) of Lemma 3.1, we assume that α is an element of type p. Then $u^{(1)}(2)\circ\alpha=u^{(p)}(2)$ and $u^{(2)}(2)\circ\alpha=u^{(2p)}(2)$. Since $m(u^{(p)}(2))=0$, we have $m(u^{(2p)}(2))+m(((1/p)\sqrt{p},0)\circ\alpha)\equiv m(u)\,(\mathrm{mod}\,l)$ for all $u\in\mathscr{R}_I^{(p)}(p)$. This and (3.11) imply that

$$m(u^{(2p)}(2))\equiv 0\,(\mathrm{mod}\,l). \tag{3.13}$$

By the congruences (3.11), (3.12) and (3.13) we have the proof. □

The following theorem shows the fullness of the Siegel units in $\mathfrak{F}_I$.

Theorem 3.1. *The functions $\hat{g}_u$ $(u\in\mathscr{R}_I^\circ)$ are independent, and the group $\mathscr{S}/k_I^\times$ has the maximal possible rank $2p-3$.*

Proof. Assume that $\prod_{u\in\mathscr{R}_I^\circ}(\hat{g}_u)^{m(u)}=1$ with $m(u)\in\boldsymbol{Z}$. Since $1=1^l$ for any prime l, we have $m(u)\equiv 0\,(\mathrm{mod}\,l)$ for all $u\in\mathscr{R}_I^\circ$ by Lemma 3.2. Since l can be any prime, we have $m(u)=0$ for all $u\in\mathscr{R}_I^\circ$. This proves the independence of the functions $\hat{g}_u$ $(u\in\mathscr{R}_I^\circ)$. Since the functions $(\hat{g}_u)^{24p}$ $(u\in\mathscr{R}_I^\circ)$ are contained in $\mathscr{S}$ (Proposition 2.2), the independence and Proposition 3.5 show that the rank of the group $\mathscr{S}/k_I^\times$ is equal to $|\mathscr{R}_I^\circ|=2p-3$. On the other hand, since the number of the cusps on the curve X_I is $2(p-1)$, it is the maximal possible value. This proves the theorem. □

The following theorem shows that the unit group $\mathscr{F}$ coincides with the group $\mathscr{S}$. It is the main theorem of this section.

Theorem 3.2. *Concerning the group $\mathscr{F}$ we have the following.*

(1) *The unit group $\mathscr{F}$ coincides with the group $\mathscr{S}$.*
(2) *The group $\mathscr{F}/k_M^\times$ has the maximal possible rank $2p-3$.*
(3) *Any function g in $\mathscr{F}$ can be written as $g = c \cdot (i\hat{g}_{w_2})^{m(w_2)} \prod_{u \in \mathscr{R}_I^\circ(p)} (g_u)^{m(u)}$ with $c \in k_M^\times$ and $m(u) \in \boldsymbol{Z}$ $(u \in \mathscr{R}_I^\circ)$, and this expression is unique.*

Proof. Since $\mathscr{F}$ contains $\mathscr{S}$, (2) follows immediately from Theorem 3.1. We prove (1). Let g be any function in $\mathscr{F}$. Then, by Theorem 3.1, some power of g can be expressed as a product of the functions $\hat{g}_u$ $(u \in \mathscr{R}_I^\circ)$ up to a constant. By the repeated use of Lemma 3.2, we obtain that g itself can be expressed as a product of the functions $\hat{g}_u$ $(u \in \mathscr{R}_I^\circ)$ up to a constant, whence $g \in \mathscr{S}$. This proves (1). (3) follows from (1), Proposition 3.5 and the independence of $\hat{g}_u$ $(u \in \mathscr{R}_I^\circ)$ (Theorem 3.1). Note that $\hat{g}_u = g_u$ for $u \in \mathscr{R}_I^\circ(p)$. □

Remark 3.1. In the next section (in Theorem 4.1) we shall prove that the integer $m(w_2)$ must be even.

Corollary 3.1. $\mathscr{F}_{\boldsymbol{C}} = \boldsymbol{C}^\times \mathscr{F}$.

Proof. Let g be any function in $\mathscr{F}_{\boldsymbol{C}}$. Then, by (2) of Theorem 3.2, some power of g belongs to $\boldsymbol{C}^\times \mathscr{F}$. This implies that there exists a non-zero constant c such that the Fourier coefficients of cg belong to k_M. Hence, we have $g \in \boldsymbol{C}^\times \mathscr{F}$. This completes the proof. □

4. Determination of the unit group on $X_1(2p)$.

In this section we determine the group $\mathscr{F}$ of the modular units in the function field $\mathfrak{F}_I$. Henceforth we assume that $p \neq 3$, therefore

$$p \neq 2, 3. \tag{4.1}$$

The reason why we exclude the case $p = 3$ is that it is exceptional and that the modular curve $X_1(6)$ coincides with the modular curve $X_0(6)$. The group of the modular units and the cuspidal class number of the curve $X_0(6)$ are already determined in [**16**].

Remark 4.1. In [**16**], the group of modular units of $X_0(6)$ is described by the functions $h_{[r]}(\tau)$ $(r \in T)$. We give the relations of these functions and our functions $\hat{g}_u$ $(u \in \mathscr{R}_I^\circ)$ in the following. Assume that $p = 3$. Since the set $\mathscr{R}_I^{(r)}(3)$ $(r \in T)$ contains only one element, we denote it by $u^{(r)}(3)$. Then we have

$$\begin{aligned} \hat{g}_{w_2}(\tau) &= c_1 \cdot h_{[3]}(\tau)\bigl\{h_{[6]}(\tau)\bigr\}^{-1}, \\ g_{u^{(r)}(3)}(\tau) &= c_2 \cdot h_{[3\circ r]}(\tau)\bigl\{h_{[r]}(\tau)\bigr\}^{-1} \end{aligned} \tag{4.2}$$

$(r \in T)$, where c_1 and c_2 are non-zero constants.

4.1. Definition of the characters Φ_u.

Let u be any element of $\mathscr{R}_I$. Since $(\hat{g}_u)^{24p}$ is an automorphic function with respect to the group $\Gamma(I)$ (Proposition 2.2), we can define the character Φ_u of $\Gamma(I)$ by

$$\hat{g}_u(\alpha(\tau)) = \Phi_u(\alpha)\hat{g}_u(\tau). \tag{4.3}$$

Let $g(\tau)$ be a function of the form

$$g(\tau) = \bigl(\hat{g}_{w_2}(\tau)\bigr)^{m(w_2)} \prod_{u \in \mathscr{R}_I(p)} (g_u(\tau))^{m(u)} \tag{4.4}$$

where $m(w_2)$ and $m(u)$ are integers. Then the function $g(\tau)$ is an automorphic function with respect to $\Gamma(I)$ if and only if the following equation holds for every $\alpha \in \Gamma(I)$:

$$\bigl\{\Phi_{w_2}(\alpha)\bigr\}^{m(w_2)} \prod_{u \in \mathscr{R}_I(p)} \{\Phi_u(\alpha)\}^{m(u)} = 1. \tag{4.5}$$

4.2. Generators of the factor group $\Gamma(I)/\Gamma(48p\mathscr{O})$.

In addition to the fact that the power $(\hat{g}_u)^{24p}$ of any function $\hat{g}_u$ $(u \in \mathscr{R}_I)$ is automorphic, the function $\hat{g}_u$ itself is an automorphic function. In fact we have the following.

Proposition 4.1.

(1) *Let u be an element of $\mathscr{R}_I(2)$. Then the function $\hat{g}_u$ is an automorphic function with respect to the principal congruence subgroup $\Gamma(48\mathscr{O})$.*

(2) *Let u be an element of $\mathscr{R}_I(p)$. Then the function $\hat{g}_u$ $(= g_u)$ is an automorphic function with respect to the principal congruence subgroup $\Gamma(12p\mathscr{O})$.*

(3) *Let u be an element of $\mathscr{R}_I(2) \cup \mathscr{R}_I(p)$. Then the function $\hat{g}_u$ is an automorphic function with respect to the principal congruence subgroup $\Gamma(48p\mathscr{O})$.*

Proof. (3) follows immediately from (1) and (2). We prove (1). By (2.31) the function $\hat{g}_u$ coincides with the function $f_r^{(2)}$ with $r = t(u)$, and it coincides with the function $f_{[r]}^{(2)}$ defined in [**16**, (2.9) in Section 2] under the condition that $M = 2p$ and $T_0 = 1$. Since the function $f_{[r]}^{(2)}$ is an automorphic function with respect to $\Gamma(48\mathscr{O})$ by [**16**, Lemma 4.1], (1) is proved. Next, we prove (2). Since our u belongs to the set A'_J in the notation of [**16**, Section 1.3] with $J = \sqrt{p}\mathscr{O}$, the function g_u is an automorphic function with respect to the group $\Gamma([2L_J^2, 12]\mathscr{O})$ by [**16**, Proposition 1.3] where $L_J = p$. Since $[2L_J^2, 12] = 12p$, (2) is proved. □

Corollary 4.1. *Let u be an element of $\mathscr{R}_I(2) \cup \mathscr{R}_I(p)$. Then the character Φ_u is trivial on the subgroup $\Gamma(48p\mathscr{O})$ of $\Gamma(I)$.*

By Corollary 4.1, in order to determine the character Φ_u, it is sufficient to determine its values at some elements of $\Gamma(I)$ which generate the factor group $\Gamma(I)/\Gamma(48p\mathscr{O})$.

For each prime factor q of $48p$, let α_q and β_q be arbitrarily chosen elements of $G(\sqrt{M})$ of type 1 so as to satisfy the following congruences:

$$\alpha_q \equiv \begin{pmatrix} 1 & \sqrt{M} \\ 0 & 1 \end{pmatrix} \bigl(\mathrm{mod}\ q^f\mathscr{O}\bigr), \quad \equiv 1_2 \bigl(\mathrm{mod}\ q^{-f}48p\mathscr{O}\bigr), \tag{4.6}$$

$$\beta_q \equiv \begin{pmatrix} 1 & 0 \\ \sqrt{M} & 1 \end{pmatrix} \bigl(\mathrm{mod}\ q^f\mathscr{O}\bigr), \quad \equiv 1_2 \bigl(\mathrm{mod}\ q^{-f}48p\mathscr{O}\bigr), \tag{4.7}$$

where $f = 4$ or 1 according as $q = 2$ or $\neq 2$.

For $q = 2$ or 3, let γ_q be an arbitrarily chosen element of $G(\sqrt{M})$ of type 1 so as to satisfy the following congruences:

$$\gamma_q \equiv \begin{pmatrix} d^{-1} & 0 \\ 0 & d \end{pmatrix} \bigl(\mathrm{mod}\ q^f\mathscr{O}\bigr), \quad \equiv 1_2 \bigl(\mathrm{mod}\ q^{-f}48p\mathscr{O}\bigr), \tag{4.8}$$

where $f = 4$ or 1 according as $q = 2$ or 3, and $d = 5$ or -1 according as $q = 2$ or 3.

Let γ'_2 be an arbitrarily chosen element of $G(\sqrt{M})$ of type 1 so as to satisfy the following congruences:

$$\gamma'_2 \equiv \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \bigl(\mathrm{mod}\ 16\mathscr{O}\bigr), \quad \equiv 1_2\ (\mathrm{mod}\ 3p\mathscr{O}). \tag{4.9}$$

Then it is easy to see that the set of the elements α_q, β_q, γ_q, γ'_2 defined above is contained in $\Gamma(I)$ and generates the factor group $\Gamma(I)/\Gamma(48p\mathscr{O})$.

4.3. The values of Φ_{w_2}.

Here we give the values of the character Φ_{w_2} at the elements α_q, β_q, γ_q, γ'_2.

Proposition 4.2. *The values of the character Φ_{w_2} at the elements α_q, β_q, γ_q, γ'_2 are given as follows*:

$$\Phi_{w_2}(\alpha_q) = \begin{cases} \exp\left[\dfrac{2\pi i}{8}\cdot 5p\right] & \text{if } q = 2, \\ \exp\left[\dfrac{2\pi i}{3}\cdot p\right] & \text{if } q = 3, \\ 1 & \text{if } q = p, \end{cases}$$

$$\Phi_{w_2}(\beta_q) = \begin{cases} \exp\left[\dfrac{2\pi i}{8}\cdot 5\right] & \text{if } q = 2, \\ \exp\left[\dfrac{2\pi i}{3}\right] & \text{if } q = 3, \\ 1 & \text{if } q = p, \end{cases}$$

$$\Phi_{w_2}(\gamma_2) = -1, \quad \Phi_{w_2}(\gamma'_2) = \Phi_{w_2}(\gamma_3) = 1.$$

Proof. The character Φ_{w_2} is already determined in [**16**]. In fact, as was seen in the proof of (1) of Proposition 4.1, the function $\hat{g}_{w_2}(\tau)$ coincides with the function $f^{(2)}_{[2p]}(\tau)$ defined in [**16**, Section 2, (2.9)] under the condition that $M = 2p$ and $T_0 = 1$, whence the character Φ_{w_2} coincides with the character $\Phi^{(2)}_{[2p]}$ defined in [**16**, Section 4.1]. In fact, the domain of the character $\Phi^{(2)}_{[2p]}$ is the subgroup Γ_{T_0} with $T_0 = 1$ which is the subgroup of $G(\sqrt{M})$ consisting of all elements of type 1, and our character Φ_{w_2} is the restriction of $\Phi^{(2)}_{[2p]}$ to the group $\Gamma(I)$.

The value $\Phi_{w_2}(\alpha_q)$ is given in [**16**, Proposition 4.1] as $\Phi^{(p)}_{\rho}(\alpha_q)$ with $\rho = [2p]$ and $p = 2$. For example, let $q = 2$. Then $\Phi_{w_2}(\alpha_2) = \Phi^{(2)}_{[2p]}(\alpha_2) = -\exp[(-2\pi i/8) \cdot (p - 2p)]$. Since $-\exp[(-2\pi i/8)(p - 2p)] = \exp[(2\pi i/8) \cdot 4p] \cdot \exp[(2\pi i/8) \cdot p] = \exp[(2\pi i/8) \cdot 5p]$, we have the desired value. The values $\Phi_{w_2}(\alpha_q)$ for other q can be obtained similarly. The value $\Phi_{w_2}(\beta_q)$ is given in [**16**, Proposition 4.1] as $\Phi^{(p)}_{\rho}(\beta_q)$ with $\rho = [2p]$ and $p = 2$. Let $q = 2$ as an example. Then $\Phi_{w_2}(\beta_2) = \Phi^{(2)}_{[2p]}(\beta_2) = -\exp[(2\pi i/8)(2-1)]$, which is equal to $\exp[(2\pi i/8)\cdot 5]$ and gives the desired value. The values $\Phi_{w_2}(\beta_q)$ for other q can also be obtained similarly. The value $\Phi_{w_2}(\gamma_q)$ $(q = 2, 3)$ is given in [**16**, Proposition 4.1] as $\Phi^{(p)}_{\rho}(\gamma_q)$ with $\rho = [2p]$ and $p = 2$, which gives the desired value. We prove that $\Phi_{w_2}(\gamma_2') = 1$. Let γ_p be the element of $G(\sqrt{M})$ defined in [**16**, p. 195]. It is an element of type 1 chosen so as to satisfy the following congruences:

$$\gamma_p \equiv \begin{pmatrix} d^{-1} & 0 \\ 0 & d \end{pmatrix} \pmod{p\mathscr{O}}, \quad \equiv 1_2 \pmod{48\mathscr{O}},$$

where d is a primitive root modulo p. (Though the element γ_p depends on the choice of d, we did not indicate its dependence in its notation because as is seen in [**16**, Proposition 4.2] the values of $\Phi_\rho^{(p)}$ do not depend on d.) Then we have $\gamma_2' \times \gamma_3 \times \gamma_p^{(p-1)/2} \equiv -1_2 \pmod{48p\mathscr{O}}$. Since $\Phi_{[2p]}^{(2)}(-1_2) = 1$ by definition and $\Phi_{[2p]}^{(2)}(\gamma_3) = \Phi_{[2p]}^{(2)}(\gamma_p) = 1$ by [**16**, Proposition 4.1], we have $\Phi_{[2p]}^{(2)}(\gamma_2') = 1$, which gives $\Phi_{w_2}(\gamma_2') = 1$. This completes the proof. □

4.4. The values of Φ_u with $u \in \mathscr{R}_I(p)$.

Let $u \in \mathscr{R}_I^{(r)}(p)$. Then $\hat{g}_u = g_u$. The value of the character Φ_u at α ($\in \Gamma(I)$) is given by

$$\Phi_u(\alpha) = \varepsilon_u(\alpha)\psi_r(\alpha) \tag{4.10}$$

by Proposition 2.1.

Let α be an element of $\Gamma(I)$ written as

$$\alpha = \begin{pmatrix} a & b\sqrt{2p} \\ c\sqrt{2p} & d \end{pmatrix} \tag{4.11}$$

where $a, b, c, d \in \boldsymbol{Z}$. Then, by (2.10), (2.16) and the definition of $\psi_r(\alpha)$, we have

$$\psi_r(\alpha) = (-1)^{(d-1)/2} \exp\left[\frac{2\pi i}{12}\{(br - cr^*)d + acr^*(1-d^2)\}\right]. \tag{4.12}$$

Lemma 4.1. *The values of ψ_r at the elements α_q, β_q, γ_q, γ_2' are given as follows.*

(1) *For $\alpha = \gamma_2, \gamma_2', \gamma_3, \alpha_p, \beta_p$, we have*

$$\psi_r(\alpha) = \begin{cases} 1 & \text{if } \alpha = \gamma_2, \gamma_3, \alpha_p, \beta_p, \\ -1 & \text{if } \alpha = \gamma_2'. \end{cases}$$

(2) *For $\alpha = \alpha_2, \alpha_3$, we have*

$$\psi_r(\alpha) = \begin{cases} \exp\left[-\dfrac{2\pi i}{4} \cdot r \right] & \text{if } \alpha = \alpha_2, \\ \exp\left[\dfrac{2\pi i}{3} \cdot r \right] & \text{if } \alpha = \alpha_3. \end{cases}$$

(3) *For $\alpha = \beta_2, \beta_3$, we have*

$$\psi_r(\alpha) = \begin{cases} \exp\left[\dfrac{2\pi i}{4} \cdot r^* \right] & \text{if } \alpha = \beta_2, \\ \exp\left[-\dfrac{2\pi i}{3} \cdot r^* \right] & \text{if } \alpha = \beta_3. \end{cases}$$

Proof. In the following we assume that the element α is written as in (4.11).

(1) In this case we have $b \equiv c \equiv 0 \pmod{12}$, whence $\psi_r(\alpha) = (-1)^{(d-1)/2}$ by (4.12). Since $d \equiv 1$ or $3 \pmod 4$ according as $\alpha = \gamma_2, \gamma_3, \alpha_p, \beta_p$ or $\alpha = \gamma_2'$, we have the desired value.

(2) In this case we have $c \equiv d-1 \equiv 0 \pmod{12}$, whence $\psi_r(\alpha) = \exp[(2\pi i/12) \cdot br]$ by (4.12). If $\alpha = \alpha_2$, we have $b = 3b_1$ with some $b_1 \in \boldsymbol{Z}$. Since $b \equiv 1 \pmod 4$, we have $b_1 \equiv -1 \pmod 4$. These imply $\psi_r(\alpha_2) = \exp[(-2\pi i/4) \cdot r]$. If $\alpha = \alpha_3$, we have $b = 4b_1$ with some $b_1 \in \boldsymbol{Z}$. Since $b \equiv 1 \pmod 3$, we have $b_1 \equiv 1 \pmod 3$. These imply $\psi_r(\alpha_3) = \exp[(2\pi i/3) \cdot r]$.

(3) In this case we have $b \equiv d-1 \equiv 0 \pmod{12}$, whence $\psi_r(\alpha) = \exp[(2\pi i/12) \cdot (-cr^*)]$ by (4.12). If $\alpha = \beta_2$, we have $c = 3c_1$ with some $c_1 \in \boldsymbol{Z}$. Since $c \equiv 1 \pmod 4$, we have $c_1 \equiv -1 \pmod 4$. These imply $\psi_r(\beta_2) = \exp[(2\pi i/4) \cdot r^*]$. If $\alpha = \beta_3$, we have $c = 4c_1$ with some $c_1 \in \boldsymbol{Z}$. Since $c \equiv 1 \pmod 3$, we have $c_1 \equiv 1 \pmod 3$. These imply $\psi_r(\beta_3) = \exp[(-2\pi i/3) \cdot r^*]$. □

The value $\varepsilon_u(\alpha)$ $(\alpha \in \Gamma(I))$ is given by

$$\varepsilon_u(\alpha) = \varepsilon(u, v) \tag{4.13}$$

with

$$v = u(\alpha - 1_2), \tag{4.14}$$

where $\varepsilon(u, v)$ is defined by (2.14) and (2.8).

Lemma 4.2. *Let $u \in \mathscr{R}_I^{(r)}(p)$ be of the form $u = ((x/p)\sqrt{r}, 0)$ $(x \in \boldsymbol{Z})$ with $r = 2p$, p. Then the values of ε_u at the elements α_q, β_q, γ_q, γ_2' are given as follows.*

(1) *For $\alpha = \alpha_2, \beta_2, \gamma_2, \gamma_2', \alpha_3, \beta_3, \gamma_3, \beta_p$, we have $\varepsilon_u(\alpha) = 1$.*
(2) *For $\alpha = \alpha_p$, we have*

$$\varepsilon_u(\alpha_p) = \begin{cases} \exp\left[\dfrac{2\pi i}{p} \cdot x^2\right] & \textit{if } r = 2p, \\ \exp\left[\dfrac{2\pi i}{p} \cdot \dfrac{1+p}{2} x^2\right] & \textit{if } r = p. \end{cases}$$

Proof. Let α be written as in (4.11). Then the element v in (4.14) is given by

$$v = \left(\frac{(a-1)x}{p}\sqrt{r}, \frac{brx}{p}\sqrt{r^*}\right),$$

whence we have $\varepsilon_u(\alpha) = \exp[\pi i \xi]$, where ξ is an element of $\boldsymbol{Q}$ satisfying

$$\xi \equiv bx \cdot \frac{r}{p} + \frac{x}{p} \cdot bx \cdot \frac{r}{p} \equiv \frac{b}{p} \cdot x\,(p+x) \cdot \frac{r}{p} \,(\mathrm{mod}\, 2\boldsymbol{Z}). \tag{4.15}$$

We note that $r/p \in \boldsymbol{Z}$.

(1) For $\alpha = \alpha_2, \beta_2, \gamma_2, \gamma_2', \alpha_3, \beta_3, \gamma_3, \beta_p$, we have $b \equiv 0 \,(\mathrm{mod}\, p)$, whence the last term in (4.15) is an integer. Since $x(p+x) \equiv 0 \,(\mathrm{mod}\, 2)$, we have $\xi \equiv 0 \,(\mathrm{mod}\, 2\boldsymbol{Z})$. Thus we have $\varepsilon_u(\alpha) = 1$.

(2) For $\alpha = \alpha_p$, we have $b \equiv 0 \,(\mathrm{mod}\, 2)$, which implies $\xi \equiv (x/p) \cdot bx \cdot (r/p)$ $(\mathrm{mod}\, 2\boldsymbol{Z})$ by the second term in (4.15). Since we also have $b \equiv 1 \,(\mathrm{mod}\, p)$, put $b = 1 + b_1 p$ with an integer b_1. Then we have $\xi \equiv (x^2/p) \cdot (r/p) + b_1 x^2 \cdot (r/p)$ $(\mathrm{mod}\, 2\boldsymbol{Z})$. If $r = 2p$, then we have $\xi \equiv 2x^2/p \,(\mathrm{mod}\, 2\boldsymbol{Z})$, which gives the desired value of $\varepsilon_u(\alpha_p)$ for the case $r = 2p$. If $r = p$, then we have $\xi \equiv x^2/p + b_1 x^2 \,(\mathrm{mod}\, 2\boldsymbol{Z})$. Since $b = 1 + b_1 p \equiv 0 \,(\mathrm{mod}\, 2)$, we have $b_1 \equiv 1 \,(\mathrm{mod}\, 2)$, whence we have $\xi \equiv x^2/p + x^2 \equiv (x^2/p)(1+p)$ $(\mathrm{mod}\, 2\boldsymbol{Z})$. This gives the desired value of $\varepsilon_u(\alpha_p)$ for the case $r = p$. □

Lemma 4.3. *Let $u \in \mathscr{R}_I^{(r)}(p)$ be of the form $u = (0, (y/p)\sqrt{r^*})$ $(y \in \boldsymbol{Z})$ with $r = 1$, 2. Then the values of ε_u at the elements α_q, β_q, γ_q, γ_2' are given as follows.*

(1) *For $\alpha = \alpha_2, \beta_2, \gamma_2, \gamma_2', \alpha_3, \beta_3, \gamma_3, \alpha_p$, we have $\varepsilon_u(\alpha) = 1$.*
(2) *For $\alpha = \beta_p$, we have*

$$\varepsilon_u(\beta_p) = \begin{cases} \exp\left[-\dfrac{2\pi i}{p} \cdot y^2 \right] & \text{if } r = 1, \\ \exp\left[-\dfrac{2\pi i}{p} \cdot \dfrac{1+p}{2} y^2 \right] & \text{if } r = 2. \end{cases}$$

Proof. Let α be written as in (4.11). Then the element v in (4.14) is given by

$$v = \left(\frac{cr^* y}{p} \sqrt{r}, \frac{(d-1)y}{p} \sqrt{r^*} \right),$$

whence we have $\varepsilon_u(\alpha) = \exp[\pi i \xi]$, where ξ is an element of $\boldsymbol{Q}$ satisfying

$$\xi \equiv cy \cdot \frac{r^*}{p} - \frac{y}{p} \cdot cy \cdot \frac{r^*}{p} \equiv \frac{c}{p} \cdot y(p-y) \cdot \frac{r^*}{p} \pmod{2\boldsymbol{Z}}. \tag{4.16}$$

We note that $r^*/p \in \boldsymbol{Z}$.

(1) For $\alpha = \alpha_2, \beta_2, \gamma_2, \gamma_2', \alpha_3, \beta_3, \gamma_3, \alpha_p$, we have $c \equiv 0 \pmod{p}$, whence the last term in (4.16) is an integer. Since $y(p-y) \equiv 0 \pmod 2$, we have $\xi \equiv 0 \pmod{2\boldsymbol{Z}}$. Thus we have $\varepsilon_u(\alpha) = 1$.

(2) For $\alpha = \beta_p$, we have $c \equiv 0 \pmod 2$, which implies $\xi \equiv (-y/p) \cdot cy \cdot (r^*/p) \pmod{2\boldsymbol{Z}}$ by the second term in (4.15). Since we also have $c \equiv 1 \pmod{p}$, put $c = 1 + c_1 p$ with an integer b_1. Then we have $\xi \equiv (-y^2/p) \cdot (r^*/p) - c_1 y^2 \cdot (r^*/p) \pmod{2\boldsymbol{Z}}$. If $r = 1$, then $r^* = 2p$, whence we have $\xi \equiv -2y^2/p \pmod{2\boldsymbol{Z}}$, which gives the desired value of $\varepsilon_u(\beta_p)$ for the case $r = 1$. If $r = 2$, then $r^* = p$, whence we have $\xi \equiv -y^2/p - c_1 y^2 \pmod{2\boldsymbol{Z}}$. Since $c = 1 + c_1 p \equiv 0 \pmod 2$, we have $c_1 \equiv 1 \pmod 2$, whence we have $\xi \equiv -y^2/p - y^2 \equiv (-y^2/p)(1+p) \pmod{2\boldsymbol{Z}}$. This gives the desired value of $\varepsilon_u(\beta_p)$ for the case $r = 2$. □

By Lemmas 4.1, 4.2 and 4.3, we have the values of the character Φ_u with $u \in \mathscr{R}_I(p)$ as follows.

Proposition 4.3. *Let $u \in \mathscr{R}_I^{(2p)}(p)$ and write $u = ((x/p)\sqrt{2p}, 0)$ $(x \in \boldsymbol{Z})$. Then the values of the character Φ_u at the elements α_q, β_q, γ_q, γ_2' are given as follows*:

$$\Phi_u(\alpha_q) = \begin{cases} -1 & \textit{if } q = 2, \\ \exp\left[-\dfrac{2\pi i}{3} \cdot p\right] & \textit{if } q = 3, \\ \exp\left[\dfrac{2\pi i}{p} \cdot x^2\right] & \textit{if } q = p, \end{cases}$$

$$\Phi_u(\beta_q) = \begin{cases} \exp\left[\dfrac{2\pi i}{4}\right] & \textit{if } q = 2, \\ \exp\left[-\dfrac{2\pi i}{3}\right] & \textit{if } q = 3, \\ 1 & \textit{if } q = p, \end{cases}$$

$$\Phi_u(\gamma_2) = \Phi_u(\gamma_3) = 1, \quad \Phi_u\bigl(\gamma_2'\bigr) = -1.$$

Proposition 4.4. *Let $u \in \mathscr{R}_I^{(p)}(p)$ and write $u = ((x/p)\sqrt{p}, 0)$ $(x \in \boldsymbol{Z})$. Then the values of the character Φ_u at the elements α_q, β_q, γ_q, γ_2' are given as follows*:

$$\Phi_u(\alpha_q) = \begin{cases} \exp\left[-\dfrac{2\pi i}{4} \cdot p\right] & \textit{if } q = 2, \\ \exp\left[\dfrac{2\pi i}{3} \cdot p\right] & \textit{if } q = 3, \\ \exp\left[\dfrac{2\pi i}{p} \cdot \dfrac{p+1}{2} x^2\right] & \textit{if } q = p, \end{cases}$$

$$\Phi_u(\beta_q) = \begin{cases} -1 & \textit{if } q = 2, \\ \exp\left[\dfrac{2\pi i}{3}\right] & \textit{if } q = 3, \\ 1 & \textit{if } q = p, \end{cases}$$

$$\Phi_u(\gamma_2) = \Phi_u(\gamma_3) = 1, \quad \Phi_u(\gamma_2') = -1.$$

Proposition 4.5. *Let $u \in \mathscr{R}_I^{(2)}(p)$ and write $u = (0, (y/p)\sqrt{p})$ $(y \in \boldsymbol{Z})$. Then the values of the character Φ_u at the elements α_q, β_q, γ_q, γ_2' are given as follows*:

$$\Phi_u(\alpha_q)=\begin{cases}-1 & \text{if } q=2,\\ \exp\left[-\dfrac{2\pi i}{3}\right] & \text{if } q=3,\\ 1 & \text{if } q=p,\end{cases}$$

$$\Phi_u(\beta_q)=\begin{cases}\exp\left[\dfrac{2\pi i}{4}\cdot p\right] & \text{if } q=2,\\ \exp\left[-\dfrac{2\pi i}{3}\cdot p\right] & \text{if } q=3,\\ \exp\left[-\dfrac{2\pi i}{p}\cdot\dfrac{p+1}{2}y^2\right] & \text{if } q=p,\end{cases}$$

$$\Phi_u(\gamma_2)=\Phi_u(\gamma_3)=1,\quad \Phi_u(\gamma_2')=-1.$$

Proposition 4.6. *Let $u\in\mathscr{R}_I^{(1)}(p)$ and write $u=(0,(y/p)\sqrt{2p})$ $(y\in\boldsymbol{Z})$. Then the values of the character Φ_u at the elements α_q, β_q, γ_q, γ_2' are given as follows*:

$$\Phi_u(\alpha_q)=\begin{cases}\exp\left[-\dfrac{2\pi i}{4}\right] & \text{if } q=2,\\ \exp\left[\dfrac{2\pi i}{3}\right] & \text{if } q=3,\\ 1 & \text{if } q=p,\end{cases}$$

$$\Phi_u(\beta_q)=\begin{cases}-1 & \text{if } q=2,\\ \exp\left[\dfrac{2\pi i}{3}\cdot p\right] & \text{if } q=3,\\ \exp\left[-\dfrac{2\pi i}{p}\cdot y^2\right] & \text{if } q=p,\end{cases}$$

$$\Phi_u(\gamma_2)=\Phi_u(\gamma_3)=1,\quad \Phi_u(\gamma_2')=-1.$$

4.5. Determination of the unit group.

Let $g(\tau)$ be a function of the form (4.4). The following theorem gives the condition that $g(\tau)$ is an automorphic function with respect to $\Gamma(I)$.

Theorem 4.1. *Let g be a function given by $g=(\hat{g}_{w_2})^{m(w_2)}\cdot\prod_{u\in\mathscr{R}_I(p)}(g_u)^{m(u)}$ with $m(w_2)$ and $m(u)$ integers. Then it is an automorphic function with respect to $\Gamma(I)$ if and only if the integers $m(w_2)$ and $m(u)$ satisfy the following conditions* (i)–(v):

(i) *$m(w_2)$ is an even integer, which we express as $m(w_2) = 2k$,*

(ii) $k + \sum_{u \in \mathscr{R}_I(p)} (t(u))^* m(u) \equiv 0 \pmod{12}$,

(iii) $\sum_{u \in \mathscr{R}_I^{(2p)}(p) \cup \mathscr{R}_I^{(p)}(p)} m(u) + p \sum_{u \in \mathscr{R}_I^{(1)}(p) \cup \mathscr{R}_I^{(2)}(p)} m(u) \equiv 0 \pmod 4$,

(iv) $\sum_{u \in \mathscr{R}_I^{(2p)}(p)} x^2 m(u) + ((p+1)/2) \sum_{u \in \mathscr{R}_I^{(p)}(p)} x^2 m(u) \equiv 0 \pmod p$,

(v) $\sum_{u \in \mathscr{R}_I^{(1)}(p)} y^2 m(u) + ((p+1)/2) \sum_{u \in \mathscr{R}_I^{(2)}(p)} y^2 m(u) \equiv 0 \pmod p$.

In the condition (iv) (*respectively* (v)) *above, it is assumed that $u = ((x/p)\sqrt{r}, 0)$ for $r = 2p, p$ with x an integer* (*respectively $u = (0, (y/p)\sqrt{r^*})$ for $r = 1, 2$ with y an integer*).

Proof. The condition that $g(\tau)$ is an automorphic function with respect to $\Gamma(I)$ is equivalent to that the equation (4.5) holds for the elements α_q, β_q, γ_q, γ_2' by Corollary 4.1 and the fact that those elements generate the factor group $\Gamma(I)/\Gamma(48p\mathscr{O})$. We prove that the relations obtained by the substitutions of the elements α_q, β_q, γ_q, γ_2' in (4.5) are equivalent to the conditions (i)–(v) in the statement. In our proof Propositions 4.2–4.6 will be used freely without any reference.

The substitution of γ_3 gives no relation about the integers $m(w_2)$ and $m(u)$ because $\Phi_{w_2}(\gamma_3) = 1$ and $\Phi_u(\gamma_3) = 1$ for all $u \in \mathscr{R}_I(p)$. The relation by the substitution of γ_2 is equivalent to (i) because $\Phi_{w_2}(\gamma_2) = -1$ and $\Phi_u(\gamma_3) = 1$ for all $u \in \mathscr{R}_I(p)$.

The relation by the substitution of β_2 is equivalent to the following:

$$\begin{aligned} &\frac{5}{8} m(w_2) + \frac{1}{4} \sum_{t(u)=2p} m(u) + \frac{1}{2} \sum_{t(u)=p} m(u) \\ &\quad + \frac{p}{4} \sum_{t(u)=2} m(u) + \frac{1}{2} \sum_{t(u)=1} m(u) \equiv 0 \pmod{\boldsymbol{Z}}. \end{aligned} \tag{4.17}$$

We use (i) and multiply (4.17) by 4. Then, since $5k \equiv k \pmod 4$ and $2 \equiv 2p \pmod 4$, we have

$$\begin{aligned} k &+ \sum_{t(u)=2p} m(u) + 2 \sum_{t(u)=p} m(u) + p \sum_{t(u)=2} m(u) + 2p \sum_{t(u)=1} m(u) \\ &\equiv 0 \pmod 4 \end{aligned} \tag{4.18}$$

which is the condition (ii) with the modulo 12 part replaced by modulo 4. The relation by the substitution of α_2 is equivalent to

$$\begin{aligned}&\frac{5}{8}pm(w_2)+\frac{1}{2}\sum_{t(u)=2p}m(u)-\frac{p}{4}\sum_{t(u)=p}m(u)\\&\quad+\frac{1}{2}\sum_{t(u)=2}m(u)-\frac{1}{4}\sum_{t(u)=1}m(u)\equiv 0\,(\mathrm{mod}\,\boldsymbol{Z}).\end{aligned}\tag{4.19}$$

Using (i) and multiplying (4.19) by 4, we have

$$\begin{aligned}&5pk+2\sum_{t(u)=2p}m(u)-p\sum_{t(u)=p}m(u)+2\sum_{t(u)=2}m(u)-\sum_{t(u)=1}m(u)\\&\quad\equiv 0\,(\mathrm{mod}\,4).\end{aligned}\tag{4.20}$$

Multiplying (4.20) by p and using the congruences $5p^2\equiv 1\,(\mathrm{mod}\,4)$, $2p\equiv 2\,(\mathrm{mod}\,4)$, $-p^2\equiv 3\,(\mathrm{mod}\,4)$, $-p\equiv 3p\,(\mathrm{mod}\,4)$, we have

$$\begin{aligned}&k+2\sum_{t(u)=2p}m(u)+3\sum_{t(u)=p}m(u)+2p\sum_{t(u)=2}m(u)+3p\sum_{t(u)=1}m(u)\\&\quad\equiv 0\,(\mathrm{mod}\,4).\end{aligned}\tag{4.21}$$

Subtracting (4.18) from (4.21) term by term gives

$$\sum_{t(u)=2p}m(u)+\sum_{t(u)=p}m(u)+p\sum_{t(u)=2}m(u)+p\sum_{t(u)=1}m(u)\equiv 0\,(\mathrm{mod}\,4),\tag{4.22}$$

which is the condition (iii). The relation by the substitution of γ_2' is equivalent to

$$\sum_{u\in\mathscr{R}_I(p)}m(u)\equiv 0\,(\mathrm{mod}\,2),$$

which follows from (4.22). The relation by the substitution of β_3 is equivalent to

$$\begin{aligned}&\frac{1}{3}m(w_2)-\frac{1}{3}\sum_{t(u)=2p}m(u)+\frac{1}{3}\sum_{t(u)=p}m(u)\\&\quad-\frac{p}{3}\sum_{t(u)=2}m(u)+\frac{p}{3}\sum_{t(u)=1}m(u)\equiv 0\,(\mathrm{mod}\,\boldsymbol{Z}).\end{aligned}\tag{4.23}$$

We use (i) and multiply (4.23) by -3. Then, by $-2k\equiv k\,(\mathrm{mod}\,3)$, $-1\equiv 2\,(\mathrm{mod}\,3)$

and $-p \equiv 2p \pmod 3$, we have

$$k + \sum_{t(u)=2p} m(u) + 2 \sum_{t(u)=p} m(u) + p \sum_{t(u)=2} m(u) + 2p \sum_{t(u)=1} m(u)$$
$$\equiv 0 \pmod 3, \tag{4.24}$$

which is the condition (ii) with the modulo 12 part replaced by modulo 3. The relation by the substitution of α_3 is equivalent to

$$\frac{p}{3} m(w_2) - \frac{p}{3} \sum_{t(u)=2p} m(u) + \frac{p}{3} \sum_{t(u)=p} m(u)$$
$$- \frac{1}{3} \sum_{t(u)=2} m(u) + \frac{1}{3} \sum_{t(u)=1} m(u) \equiv 0 \pmod{\boldsymbol{Z}}. \tag{4.25}$$

Using (i) and multiplying (4.25) by 3, we have

$$2pk - p \sum_{t(u)=2p} m(u) + p \sum_{t(u)=p} m(u) - \sum_{t(u)=2} m(u) + \sum_{t(u)=1} m(u)$$
$$\equiv 0 \pmod 3. \tag{4.26}$$

Multiplying (4.26) by $-p$ and using the congruences $-2p^2 \equiv 1 \pmod 3$, $(-p)^2 \equiv 1 \pmod 3$, $-p^2 \equiv 2 \pmod 3$ and $-p \equiv 2p \pmod 3$, we have the congruence (4.24). Summing up the arguments above, we see that the relations obtained by the substitutions of the elements α_2, α_3, β_2, β_3, γ_2, γ_2' and γ_3 are equivalent to the conditions (i)–(iii).

The relation by the substitution of α_p is equivalent to

$$\frac{1}{p} \sum_{t(u)=2p} x^2 m(u) + \frac{p+1}{2p} \sum_{t(u)=p} x^2 m(u) \equiv 0 \pmod{\boldsymbol{Z}}. \tag{4.27}$$

Multiplying (4.27) by p, we obtain the congruence in the condition (iv). The relation by the substitution of β_p is equivalent to

$$-\frac{p+1}{2p} \sum_{t(u)=2} y^2 m(u) - \frac{1}{p} \sum_{t(u)=1} y^2 m(u) \equiv 0 \pmod{\boldsymbol{Z}}. \tag{4.28}$$

Multiplying (4.28) by $-p$, we obtain the congruence in the condition (v). This completes the proof. □

Now we can determine the group $\mathscr{F}$ of the modular units in the function field $\mathfrak{F}_I$. The following is the main theorem in this section.

Theorem 4.2. *The group $\mathscr{F}$ of the modular units in the function field $\mathfrak{F}_I$ consists of all functions g of the form*

$$g = c(g_{w_2})^k \prod_{u \in \mathscr{R}_I(p)} (g_u)^{m(u)},$$

where $c \in k_M^\times$, and k and $m(u)$ are integers satisfying the relations (ii)–(v) *of Theorem* 4.1.

Let u_1 (respectively u_2) be any element of $\mathscr{R}_I(p)$ with $t(u_1) = 1$ or p (respectively $t(u_2) = 2$ or $2p$). Then in the expression of g we can make $m(u_1)$ and $m(u_2)$ equal to 0, *and in that case the integers k and $m(u)$ $(u \in \mathscr{R}_I(p))$ are uniquely determined by g.*

Proof. This follows immediately from Theorems 3.2 and 4.1. □

Remark 4.2. Since $\hat{g}_{w_2} = f_{2p}^{(2)}$ by (2.31), the function $g_{w_2} = (\hat{g}_{w_2})^2$ can be expressed by the Dedekind η-function $\eta(\tau)$: $g_{w_2}(\tau) = -H^2(p\tau)H^{-2}(2p\tau)$, where $H(\tau) = \eta(\tau/\sqrt{2p})$.

5. Computation of the cuspidal class number.

In this section we determine the cuspidal class number of the modular curve $X_1(2p)$.

5.1. The image I_P of the principal divisors in the group ring.

Let $\varphi : \mathscr{D} \cong R$ be the isomorphism (2.23). In this subsection we determine the image $\varphi(\operatorname{div}(\mathscr{F}))$, which we denote by I_P, of the principal divisors $\operatorname{div}(\mathscr{F})$ of the modular units in $\mathfrak{F}_I$. Let R_0 be the subgroup of R of all elements of degree 0. Then $I_P = \varphi(\operatorname{div}(\mathscr{F}))$ is an additive subgroup of R_0.

By Theorem 4.2 any function g in $\mathscr{F}$ is a product of the functions g_{w_2} and g_u with $u \in \mathscr{R}_I(p)$ up to a constant. The set $\mathscr{R}_I(p)$ is a complete set of representatives of $\mathscr{A}_I'(p)$. By Proposition 2.6 the set $\mathscr{A}_I'(p)$ is an orbit of $C_I(\pm)$ with $\mathscr{A}_I'(p) = [w_p]C_I(\pm)$, and by (2) of Proposition 2.9 the stabilizer $St([w_p])$ of $[w_p]$ is trivial because $p^* = 2$ and $(\boldsymbol{Z}/2\boldsymbol{Z})^\times = 1$. Hence the sets $C_I(\pm)$ and $\mathscr{R}_I(p)$ correspond bijectively by the mapping $\alpha \longmapsto w_p \circ \alpha$. (For the definition of the product $w_p \circ \alpha$, see (3.5).)

Let α be any element of $C_I(\pm)$ of type r. Let $a(\alpha)$ and $b(\alpha)$ be integers such that α can be represented by the matrix

$$\begin{pmatrix} a(\alpha)\sqrt{r} & b(\alpha)\sqrt{r^*} \\ b(\alpha)\sqrt{r^*} & a(\alpha)\sqrt{r} \end{pmatrix}. \tag{5.1}$$

Although such integers $a(\alpha)$ and $b(\alpha)$ are not unique, the residue classes $a(\alpha) \pmod{r^*}$ and $b(\alpha) \pmod{r}$ are uniquely determined up to the multiplication by ± 1. In particular, the element α determines the residue class $a(\alpha)^2 (\operatorname{mod} p)$ (respectively $b(\alpha)^2 (\operatorname{mod} p)$) uniquely when $r = 1, 2$ (respectively $r = p, 2p$).

Theorem 5.1. *Let $\varphi : \mathscr{D} \cong R$ be the isomorphism* (2.23). *Let* $\operatorname{div}(\mathscr{F})$ *be the group of the principal divisors of the modular units in $\mathfrak{F}_I$. Then the image $I_P = \varphi(\operatorname{div}(\mathscr{F}))$ is the subgroup of R_0 consisting of all elements*

$$2k\theta_2 + \Bigg\{ \sum_{\alpha \in C_I(\pm)} m(\alpha)\alpha \Bigg\} \theta_p, \tag{5.2}$$

where k and $m(\alpha)$ are integers such that the following congruences (i)–(iv) *hold*:

(i) $k + \sum_{\alpha \in C_I(\pm)} t(\alpha) m(\alpha) \equiv 0 \pmod{12}$,
(ii) $\sum_{\alpha \in C_I^{(1)}(\pm) \cup C_I^{(2)}(\pm)} m(\alpha) + p \sum_{\alpha \in C_I^{(p)}(\pm) \cup C_I^{(2p)}(\pm)} m(\alpha) \equiv 0 \pmod{4}$,
(iii) $\sum_{\alpha \in C_I^{(1)}(\pm)} a(\alpha)^2 m(\alpha) + 2 \sum_{\alpha \in C_I^{(2)}(\pm)} a(\alpha)^2 m(\alpha) \equiv 0 \pmod{p}$,
(iv) $\sum_{\alpha \in C_I^{(2p)}(\pm)} b(\alpha)^2 m(\alpha) + 2 \sum_{\alpha \in C_I^{(p)}(\pm)} b(\alpha)^2 m(\alpha) \equiv 0 \pmod{p}$.

Proof. Let g be any function in $\mathscr{F}$. Then by Theorem 4.2 we have

$$g = c(g_{w_2})^k \prod_{u \in \mathscr{R}_I(p)} (g_u)^{m(u)},$$

where k and $m(u)$ are integers satisfying (ii)–(v) of Theorem 4.1. Let $u = w_p \circ \alpha$ with $\alpha \in C_I(\pm)$. Since the mapping $\alpha \longmapsto w_p \circ \alpha$ between $C_I(\pm)$ and $\mathscr{R}_I(p)$ is bijective, we can express $m(u)$ as $m(\alpha)$. By (2.41) and (2.42), we have $\varphi(\operatorname{div}(g_{w_2}))$ $= 2\theta_2$ and $\varphi(\operatorname{div}(g_u)) = \alpha\theta_p$, hence

$$\varphi(\operatorname{div}(g)) = 2k\theta_2 + \Bigg\{ \sum_{\alpha \in C_I(\pm)} m(\alpha)\alpha \Bigg\} \theta_p.$$

Since $(t(u))^* = t(\alpha)$, the relation (ii) (respectively (iii)) of Theorem 4.1 coincides with the relation (i) (respectively (ii)) in our statement. When $t(u)(= r) = 2p$

or p, write $u = ((x/p)\sqrt{r}, 0)$ with x an integer. It is easy to see that $x^2 \equiv a(\alpha)^2 \pmod{p}$ or $4a(\alpha)^2 \pmod{p}$ according as $r = 2p$ or p. When $r = p$, we have $((p+1)/2)x^2 \equiv 2(p+1)a(\alpha)^2 \equiv 2a(\alpha)^2 \pmod{p}$. These imply that the relation (iv) of Theorem 4.1 coincides with the relation (iii) in our statement. When $t(u)(= r) = 1$ or 2, write $u = (0, (y/p)\sqrt{r^*})$ with y an integer. Then it is easy to see that $y^2 \equiv b(\alpha)^2 \pmod{p}$ or $4b(\alpha)^2 \pmod{p}$ according as $r = 1$ or 2. When $r = 2$, we have $((p+1)/2)y^2 \equiv 2(p+1)b(\alpha)^2 \equiv 2b(\alpha)^2 \pmod{p}$. These imply that the relation (v) of Theorem 4.1 coincides with the relation (iv) in our statement. Thus $\varphi(\mathrm{div}(g))$ satisfies the conditions (i)–(iv). Conversely, by the arguments above, it is obvious that any element (5.2) of R satisfying the conditions (i)–(iv) of our statement can be expressed as $\varphi(\mathrm{div}(g))$ with $g \in \mathscr{F}$. This completes the proof.

□

Remark 5.1. The subgroup I_P of R is an ideal of R. In fact, for any modular unit $f \in \mathscr{F}$ and any element $\alpha \in C_I(\pm)$, the divisor $\mathrm{div}(f^{\sigma(\alpha)})$ of $f^{\sigma(\alpha)}$ ($\in \mathfrak{F}_I$) is supported only on the cuspidal prime divisors since any conjugate of a cuspidal prime divisor is itself a cuspidal prime divisor (cf. Section 2.6). Hence $f^{\sigma(\alpha)}$ is also a modular unit. The relation $\alpha\,\mathrm{div}(f) = \mathrm{div}(f^{\sigma(\alpha)})$ follows from the argument similar to the one in the proof of Proposition 2.5. This proves that I_P is an ideal of R.

5.2. The subgroup $24\boldsymbol{Z}\theta_2 + I_{12}\theta_p$ of I_P.

By Theorem 5.1 the cuspidal divisor class group $\mathscr{C}$ (3.2) is isomorphic to the factor group R_0/I_P:

$$\mathscr{C} \cong R_0/I_P. \tag{5.3}$$

We denote by h the cuspidal class number of the modular curve $X_1(2p)$. Then we have

$$h = [R_0 : I_P]. \tag{5.4}$$

In the group I_P the θ_2-part and θ_p-part affect each other by the relation (i) of Theorem 5.1. We introduce the subgroup I_{12} of R in order to separate the two parts as follows. Let I_{12} be the subgroup of R consisting of all elements $\sum_{\alpha \in C_I(\pm)} m(\alpha)\alpha$ of R with $m(\alpha) \in \boldsymbol{Z}$ such that the integers $m(\alpha)$ satisfy the following condition (i*) and the conditions (ii)–(iv) of Theorem 5.1:

$$\text{(i*)} \qquad \sum_{\alpha \in C_I(\pm)} t(\alpha)m(\alpha) \equiv 0 \pmod{12}. \tag{5.5}$$

We shall prove that $24\boldsymbol{Z}\theta_2 + I_{12}\theta_p$ is a subgroup of I_P of index 12, and that it is a direct sum.

Remark 5.2. It can be proved that the subgroup I_{12} is an ideal of R. Since this fact is not used in this paper, we omit the proof.

Let $R_{\boldsymbol{C}} = R \otimes \boldsymbol{C}$ be the group ring of $C_I(\pm)$ over $\boldsymbol{C}$. Let χ be any character of $C_I(\pm)$, and let e_χ be the elementary idempotent defined by

$$e_\chi = \frac{1}{|C_I(\pm)|} \sum_{\alpha \in C_I(\pm)} \chi(\alpha)\alpha^{-1}. \tag{5.6}$$

As is well-known these elements e_χ constitute a basis of $R_{\boldsymbol{C}}$ and satisfy the orthogonality relation.

We determine the e_χ-components of θ_2 and θ_p. Let ϕ be the natural homomorphism of $(\boldsymbol{Z}/p\boldsymbol{Z})^\times$ to $(\boldsymbol{Z}/2p\boldsymbol{Z})^\times/\pm 1$ defined by

$$\phi : (\boldsymbol{Z}/p\boldsymbol{Z})^\times \cong (\boldsymbol{Z}/2p\boldsymbol{Z})^\times \to (\boldsymbol{Z}/2p\boldsymbol{Z})^\times/\pm 1. \tag{5.7}$$

For any character χ of $C_I(\pm)$ we define the character ψ_χ of $(\boldsymbol{Z}/p\boldsymbol{Z})^\times$ by

$$\psi_\chi(a) = \chi\left(\begin{pmatrix} \phi(a) & 0 \\ 0 & \phi(a) \end{pmatrix} \right). \tag{5.8}$$

It is obvious that $\psi_\chi(-1) = 1$.

Let ψ be a non-trivial character of $(\boldsymbol{Z}/p\boldsymbol{Z})^\times$. Let $B_2(X)$ be the second Bernoulli polynomial (cf. (2.6)). Let $B_{2,\psi}$ be the generalized Bernoulli number associated to ψ which is defined by

$$B_{2,\psi} = p \sum_{a=1}^{p-1} \psi(a) B_2\left(\frac{a}{p}\right). \tag{5.9}$$

Then the e_χ-components of θ_p are given as follows.

Proposition 5.1. *Let χ be a character of $C_I(\pm)$, and put $\psi = \psi_\chi$. We denote by $\overline{\psi}$ the complex conjugate of ψ. Let* [2] *and* [p] *be the elements of $C_I(\pm)$ defined by* (2.45). *Then we have*

$$\theta_p e_\chi = \begin{cases} \dfrac{1}{4}(2+\chi([2]))B_{2,\overline{\psi}}e_\chi & \textit{if } \chi \textit{ is non-trivial on } C_I^{(1)}(\pm), \\ -\dfrac{p-1}{24}(2+\chi([2]))(1-\chi([p]))e_\chi & \textit{if } \chi \textit{ is trivial on } C_I^{(1)}(\pm). \end{cases}$$

Proof. Let $f(\alpha)$ be the function on $C_I(\pm)$ defined by $\theta_p = \sum_{\alpha\in C_I(\pm)} f(\alpha)\alpha^{-1}$. Then we have

$$\theta_p e_\chi = \Big\{\sum_{\alpha\in C_I(\pm)} f(\alpha)\chi(\alpha)^{-1}\Big\}e_\chi.$$

The values of $f(\alpha)$ are given in (2) of Proposition 3.1.

Let $t(\alpha)=1$. Then α can be represented by a matrix of the form $\left(\begin{smallmatrix} a(\alpha) & 0 \\ 0 & a(\alpha)\end{smallmatrix}\right)$ with $a(\alpha)\in \boldsymbol{Z}$. We have $f(\alpha) = pB_2(\langle a(\alpha)/p\rangle)$ and $\chi(\alpha)^{-1} = \overline{\psi}(a(\alpha))$. If α runs through $C_I^{(1)}(\pm)$, the class of $a(\alpha)$ runs through all elements of $(\boldsymbol{Z}/p\boldsymbol{Z})^\times/\pm 1$. This implies that $\sum_{\alpha\in C_I^{(1)}(\pm)} f(\alpha)\chi(\alpha)^{-1} = (1/2)B_{2,\overline{\psi}}$ or $-(p-1)/12$ according as χ is non-trivial or trivial on $C_I^{(1)}(\pm)$ respectively.

Let $t(\alpha) = 2$. Then α can be represented by a matrix of the form $\left(\begin{smallmatrix} a(\alpha)\sqrt{2} & \sqrt{p} \\ \sqrt{p} & a(\alpha)\sqrt{2}\end{smallmatrix}\right)$ with $a(\alpha)\in\boldsymbol{Z}$, and $f(\alpha) = (p/2)B_2(\langle 2a(\alpha)/p\rangle)$. Put $\beta = \alpha[2]$. Then β is represented by the matrix $\left(\begin{smallmatrix} 2a(\alpha)+p & 0 \\ 0 & 2a(\alpha)+p\end{smallmatrix}\right)$, and $\chi(\alpha)^{-1} = \chi(\beta)^{-1}\chi([2]) = \overline{\psi}(2a(\alpha))\chi([2])$. If α runs through $C_I^{(2)}(\pm)$, the class of $2a(\alpha)$ runs through all elements of $(\boldsymbol{Z}/p\boldsymbol{Z})^\times/\pm 1$. This implies that $\sum_{\alpha\in C_I^{(2)}(\pm)} f(\alpha)\chi(\alpha)^{-1} = (1/4)B_{2,\overline{\psi}}\chi([2])$ or $-((p-1)/24)\chi([2])$ according as χ is non-trivial or trivial on $C_I^{(1)}(\pm)$ respectively.

Let $t(\alpha) = p$. Then $f(\alpha) = 1/6$. Put $\beta = \alpha[p]$. Then $\chi(\alpha)^{-1} = \chi(\beta)^{-1}\chi([p])$, and if α runs through $C_I^{(p)}(\pm)$, β runs through $C_I^{(1)}(\pm)$. This implies that $\sum_{\alpha\in C_I^{(p)}(\pm)} f(\alpha)\chi(\alpha)^{-1} = 0$ or $((p-1)/12)\chi([p])$ according as χ is non-trivial or trivial on $C_I^{(1)}(\pm)$ respectively.

Let $t(\alpha) = 2p$. Then $f(\alpha) = 1/12$. Put $\beta = \alpha[2][p]$. Then $\chi(\alpha)^{-1} = \chi(\beta)^{-1}\chi([2])\chi([p])$, and if α runs through $C_I^{(2p)}(\pm)$, β runs through $C_I^{(1)}(\pm)$. This implies that $\sum_{\alpha\in C_I^{(2p)}(\pm)} f(\alpha)\chi(\alpha)^{-1} = 0$ or $((p-1)/24)\chi([2])\chi([p])$ according as χ is non-trivial or trivial on $C_I^{(1)}(\pm)$ respectively.

Summing up the results above, we have

$$\sum_{\alpha\in C_I(\pm)} f(\alpha)\chi(\alpha)^{-1} = \frac{1}{2}B_{2,\overline{\psi}} + \frac{1}{4}B_{2,\overline{\psi}}\chi([2]) = \frac{1}{4}(2+\chi([2]))B_{2,\overline{\psi}}$$

if χ is non-trivial on $C_I^{(1)}(\pm)$, and

$$\begin{aligned}&\sum_{\alpha\in C_I(\pm)} f(\alpha)\chi(\alpha)^{-1}\\ &\quad= -\frac{p-1}{12} - \frac{p-1}{24}\chi([2]) + \frac{p-1}{12}\chi([p]) + \frac{p-1}{24}\chi([2])\chi([p])\\ &\quad= -\frac{p-1}{24}(2+\chi([2]))(1-\chi([p]))\end{aligned}$$

if χ is trivial on $C_I^{(1)}(\pm)$. This completes the proof. □

Corollary 5.1. *Let χ and $[p]$ be as in Proposition* 5.1.

(1) *If χ is non-trivial on $C_I^{(1)}(\pm)$, then $\theta_p e_\chi \neq 0$.*
(2) *If χ is trivial on $C_I^{(1)}(\pm)$, then $\theta_p e_\chi \neq 0$ or $= 0$ according as $\chi([p]) \neq 1$ or $= 1$ respectively.*

Proof.

(1) In this case the character ψ (also $\overline{\psi}$) is non-trivial. Since it is well-known that $B_{2,\overline{\psi}} \neq 0$ if $\overline{\psi}$ is non-trivial, we have the proof by Proposition 5.1.
(2) This follows immediately from Proposition 5.1. □

Let χ be anyone of the four characters of $C_I(\pm)$ which are trivial on $C_I^{(1)}(\pm)$. If χ satisfies the condition

$$\chi([2]) = -1 \quad\text{and}\quad \chi([p]) = 1, \tag{5.10}$$

then we write $\chi = \chi_{(2)}$. If χ satisfies the condition

$$\chi([2]) = 1 \quad\text{and}\quad \chi([p]) = -1, \tag{5.11}$$

then we write $\chi = \chi_{(p)}$. Also, we denote the product $\chi_{(2)}\chi_{(p)}$ by $\chi_{(2,p)}$ and the trivial character of $C_I(\pm)$ by $\chi_{(0)}$.

The e_χ-components of θ_2 are given as follows.

Proposition 5.2. *Let χ be a character of $C_I(\pm)$. Then*

$$\theta_2 e_\chi = \begin{cases} -\dfrac{p-1}{24}(p+\chi([p]))e_\chi & \textit{if } \chi = \chi_{(2)} \textit{ or } \chi_{(2,p)},\\ 0 & \textit{otherwise.}\end{cases}$$

Proof. By (1) of Proposition 3.1 and the fact that $C_I^{(r)}(\pm) = [r]C_I^{(1)}(\pm)$ for $r = 2, p$ and $C_I^{(2p)}(\pm) = [2][p]C_I^{(1)}(\pm)$, we have

$$\begin{aligned}\theta_2 &= \frac{1}{24}(-p + p[2] - [p] + [2][p]) \sum_{\alpha \in C_I^{(1)}(\pm)} \alpha \\ &= -\frac{1}{24}(1 - [2])(p + [p]) \sum_{\alpha \in C_I^{(1)}(\pm)} \alpha.\end{aligned}$$

By this equation we have

$$\theta_2 e_\chi = -\frac{1}{24}(1 - \chi([2]))(p + \chi([p]))\Bigl\{\sum_{\alpha \in C_I^{(1)}(\pm)} \chi(\alpha)\Bigr\} e_\chi.$$

Let χ be non-trivial on $C_I^{(1)}(\pm)$. Then $\sum_{\alpha \in C_I^{(1)}(\pm)} \chi(\alpha) = 0$, therefore $\theta_2 e_\chi = 0$. Let χ be trivial on $C_I^{(1)}(\pm)$ and $\chi([2]) = 1$. Then $\chi = \chi_{(0)}$ or $\chi_{(p)}$, and $\theta_2 e_\chi = 0$. Let $\chi = \chi_{(2)}$ or $\chi_{(2,p)}$. Then $\chi([2]) = -1$. Since $|C_I^{(1)}(\pm)| = (1/2)(p-1)$, we have $\theta_2 e_\chi = -((p-1)/24)(p + \chi([p]))e_\chi$. This completes the proof. □

The following proposition suggests that it is easier to consider the subgroup $24\boldsymbol{Z}\theta_2 + I_{12}\theta_p$ of I_P than I_P itself.

Proposition 5.3.

(1) *The group* $24\boldsymbol{Z}\theta_2 + I_{12}\theta_p$ *is a subgroup of* I_P, *and*

$$I_P/(24\boldsymbol{Z}\theta_2 + I_{12}\theta_p) \cong \boldsymbol{Z}/12\boldsymbol{Z}.$$

(2) *We have* $24\boldsymbol{Z}\theta_2 \cap I_{12}\theta_p = 0$, *therefore* $24\boldsymbol{Z}\theta_2 + I_{12}\theta_p$ *is a direct sum.*

Proof.

(1) It is obvious that the group $24\boldsymbol{Z}\theta_2 + I_{12}\theta_p$ is contained in I_P. Let $\eta = 2k\theta_2 + \xi\theta_p$ be any element of I_P with $k \in \boldsymbol{Z}$ and $\xi \in R$. By Corollary 5.1 and Proposition 5.2 we have $\eta e_{\chi_{(2)}} = 2k\theta_2 e_{\chi_{(2)}} + \xi\theta_p e_{\chi_{(2)}} = 2k\{-(1/24)(p^2-1)\}e_{\chi_{(2)}}$. This implies that the integer k is uniquely determined by η. Let $\varphi(\eta)$ be the residue class of k modulo 12. Then we have a homomorphism $\varphi : I_P \to \boldsymbol{Z}/12\boldsymbol{Z}$. Since k and ξ satisfy the conditions (i)–(iv) of Theorem 5.1, it is obvious that $\varphi^{-1}(0) = 24\boldsymbol{Z}\theta_2 + I_{12}\theta_p$. We prove that φ is surjective. Put $\eta_1 = 2p^2\theta_2 + p^2(1-[2])\theta_p$. It is easy to see that $\eta_1 \in I_P$. Since $p \neq 2, 3$, we have $\varphi(\eta_1) = p^2 (\mathrm{mod}\, 12) = 1 (\mathrm{mod}\, 12)$.

This implies that φ is surjective. Thus the proof is completed.

(2) Let η be any element of $24\boldsymbol{Z}\theta_2 \cap I_{12}\theta_p$. Then $\eta = 2k\theta_2 = \xi\theta_p$ with $k \in \boldsymbol{Z}$ and $\xi \in I_{12}$. Since $\eta = 2k\theta_2 + 0 \cdot \theta_p = 2 \cdot 0 \cdot \theta_2 + \xi\theta_p$, we have $k = 0$ by the uniqueness of k proved in (1). Therefore we have $\eta = 0$. This completes the proof. □

5.3. Extending $I_{12}\theta_p$ to $R_{0,0}$.

By (5.4) and Proposition 5.3 we have

$$h = \frac{1}{12}\big[R_0 : (24\boldsymbol{Z}\theta_2 + I_{12}\theta_p)\big]. \tag{5.12}$$

Since θ_p satisfies $\theta_p e_{\chi_{(0)}} = \theta_p e_{\chi_{(2)}} = 0$ by Corollary 5.1, the group $I_{12}\theta_p$ is contained in the subgroup $R_{0,0}$ of R which consists of all elements $\xi \in R$ satisfying

$$\xi e_{\chi_{(0)}} = \xi e_{\chi_{(2)}} = 0. \tag{5.13}$$

We consider here the extension $24\boldsymbol{Z}\theta_2 + R_{0,0}$ of $24\boldsymbol{Z}\theta_2 + I_{12}\theta_p$.

Let χ be any character of $C_I(\pm)$. Let $\xi = \sum_{\alpha \in C_I(\pm)} m(\alpha)\alpha$ be any element of $R_{\boldsymbol{C}}$ with $m(\alpha) \in \boldsymbol{C}$. We denote by $\chi(\xi)$ the number defined by

$$\chi(\xi) = \sum_{\alpha \in C_I(\pm)} m(\alpha)\chi(\alpha). \tag{5.14}$$

Then $\xi e_\chi = \chi(\xi)e_\chi$. The mapping $\xi \longmapsto \chi(\xi)$ defines a $\boldsymbol{C}$-algebra homomorphism $\chi : R_{\boldsymbol{C}} \to \boldsymbol{C}$. We denote by $\xi^{(r)}$ $(r \in T)$ the element of $R_{\boldsymbol{C}}$ defined by

$$\xi^{(r)} = \sum_{\alpha \in C_I^{(r)}(\pm)} m(\alpha)\alpha. \tag{5.15}$$

Proposition 5.4. *Let $R_{0,0}$ be as above. Then we have the following.*

(1) $I_{12}\theta_p \subset R_{0,0} \subset R_0$.
(2) $24\boldsymbol{Z}\theta_2 \cap R_{0,0} = 0$, *therefore the sum* $24\boldsymbol{Z}\theta_2 + R_{0,0}$ *is a direct sum.*
(3) $(24\boldsymbol{Z}\theta_2 + R_{0,0})/(24\boldsymbol{Z}\theta_2 + I_{12}\theta_p) \cong R_{0,0}/I_{12}\theta_p$.
(4) $R_0/(24\boldsymbol{Z}\theta_2 + R_{0,0}) \cong \boldsymbol{Z}/((1/2)(p^2-1))\boldsymbol{Z}$.

Proof.

(1) The inclusion $I_{12}\theta_p \subset R_{0,0}$ is obvious by the definition of $R_{0,0}$. Let ξ be any element of $R_{0,0}$. Then $\xi e_{\chi_{(0)}} = 0$. Since $\xi e_{\chi_{(0)}} = \deg(\xi)e_{\chi_{(0)}}$, we have $\deg(\xi) = 0$, whence $\xi \in R_0$. This proves (1).

(2) Let ξ be any element of $24\boldsymbol{Z}\theta_2 \cap R_{0,0}$. Then $\xi = 24k\theta_2$ with $k \in \boldsymbol{Z}$. By Proposition 5.2 we have $\xi e_{\chi_{(2)}} = 24k\theta_2 e_{\chi_{(2)}} = -k(p^2-1)e_{\chi_{(2)}}$. On the other hand, by the definition of $R_{0,0}$, we have $\xi e_{\chi_{(2)}} = 0$. This gives $k = 0$, hence $\xi = 0$. This proves (2).

(3) This follows immediately from (2) of Proposition 5.3 and (1), (2) above.

(4) Let ξ be any element of R_0. We have $\xi e_{\chi_{(2)}} = \chi_{(2)}(\xi) e_{\chi_{(2)}}$, where

$$\chi_{(2)}(\xi) = \deg \xi^{(1)} - \deg \xi^{(2)} + \deg \xi^{(p)} - \deg \xi^{(2p)}. \tag{5.16}$$

On the other hand, since $\xi \in R_0$, we have

$$\deg \xi = \deg \xi^{(1)} + \deg \xi^{(2)} + \deg \xi^{(p)} + \deg \xi^{(2p)} = 0. \tag{5.17}$$

By (5.16) and (5.17) we have

$$\chi_{(2)}(\xi) = 2\big(\deg \xi^{(1)} + \deg \xi^{(p)}\big) \in 2\boldsymbol{Z}.$$

Let $\varphi(\xi)$ be the residue class of $(1/2)\chi_{(2)}(\xi)$ $(\in \boldsymbol{Z})$ modulo $(1/2)(p^2-1)$. Then φ is a homomorphism from R_0 to $\boldsymbol{Z}/((1/2)(p^2-1))\boldsymbol{Z}$. First we prove that φ is surjective. In fact, put $\xi_1 = 1 - [2]$ $(\in R_0)$. Then we have $\varphi(\xi_1) = 1 \,(\mathrm{mod}((1/2) \cdot (p^2-1)))$, which proves that φ is surjective. Next we prove that the kernel of φ coincides with $24\boldsymbol{Z}\theta_2 + R_{0,0}$. Let $\eta = 24k\theta_2 + \xi$ be any element of $24\boldsymbol{Z}\theta_2 + R_{0,0}$ with $k \in \boldsymbol{Z}$ and $\xi \in R_{0,0}$. Then $\eta e_{\chi_{(2)}} = 24k\theta_2 e_{\chi_{(2)}} + \xi e_{\chi_{(2)}} = -k(p^2-1)e_{\chi_{(2)}}$ by Proposition 5.2 and (5.13). This implies that $(1/2)\chi_{(2)}(\eta) = -k((1/2)(p^2-1))$ and $\varphi(\eta) = 0$, hence we have $24\boldsymbol{Z}\theta_2 + R_{0,0} \subset \varphi^{-1}(0)$. Conversely, let η be any element of $\varphi^{-1}(0)$. Then $(1/2)\chi_{(2)}(\eta) = k((1/2)(p^2-1))$ with some $k \in \boldsymbol{Z}$. Put $\xi = \eta + 24k\theta_2$. Then we have $\xi e_{\chi_{(2)}} = \eta e_{\chi_{(2)}} + 24k\theta_2 e_{\chi_{(2)}} = k(p^2-1)e_{\chi_{(2)}} - k(p^2-1)e_{\chi_{(2)}} = 0$, which implies that $\xi \in R_{0,0}$ and $\eta \in 24\boldsymbol{Z}\theta_2 + R_{0,0}$. Thus we have $\varphi^{-1}(0) \subset 24\boldsymbol{Z}\theta_2 + R_{0,0}$, therefore $\varphi^{-1}(0) = 24\boldsymbol{Z}\theta_2 + R_{0,0}$. This gives the isomorphism $R_0/(24\boldsymbol{Z}\theta_2 + R_{0,0}) \cong \boldsymbol{Z}/((1/2)(p^2-1))\boldsymbol{Z}$, which proves (4). □

5.4. The invertible element θ'.

By (5.12) and Proposition 5.4 we have

$$\begin{aligned} h &= \frac{1}{12}\big[R_0 : (24\boldsymbol{Z}\theta_2 + R_{0,0})\big]\big[(24\boldsymbol{Z}\theta_2 + R_{0,0}) : (24\boldsymbol{Z}\theta_2 + I_{12}\theta_p)\big] \\ &= \frac{1}{12} \cdot \frac{1}{2}(p^2-1) \cdot \big[R_{0,0} : I_{12}\theta_p\big] = \frac{p^2-1}{24}\big[R_{0,0} : I_{12}\theta_p\big]. \end{aligned} \tag{5.18}$$

The element θ_p is not invertible in $R_{\boldsymbol{C}}$ because the e_χ-components for $\chi = \chi_{(0)}$

and $\chi = \chi_{(2)}$ are 0 by Corollary 5.1. We want an element θ' which has the same non-zero e_χ-components as θ_p and is invertible. Since the e_χ-component of θ_p for any $\chi \neq \chi_{(0)}, \chi_{(2)}$ is non-zero by Corollary 5.1, it is sufficient to put $\theta' = \theta_p - s$ where s is an element which has only two non-zero e_χ-components for $\chi = \chi_{(0)}$ and $\chi = \chi_{(2)}$.

We denote by μ the element of R defined by

$$\mu = \sum_{\alpha \in C_I(\pm)} \alpha. \tag{5.19}$$

Then we have the following lemma that gives all elements of R such that they have only two non-zero e_χ-components for $\chi = \chi_{(0)}$ and $\chi = \chi_{(2)}$ at most.

Lemma 5.1. $R \cap \big(\boldsymbol{C} e_{\chi_{(0)}} + \boldsymbol{C} e_{\chi_{(2)}}\big) = \boldsymbol{Z}\big(\mu^{(1)} + \mu^{(p)}\big) + \boldsymbol{Z}\big(\mu^{(2)} + \mu^{(2p)}\big)$.

Proof. Let $\xi = x e_{\chi_{(0)}} + y e_{\chi_{(2)}}$ with $x, y \in \boldsymbol{C}$ be any element of $R \cap \big(\boldsymbol{C} e_{\chi_{(0)}} + \boldsymbol{C} e_{\chi_{(2)}}\big)$. By the definition of $e_{\chi_{(0)}}$ and $e_{\chi_{(2)}}$ we have

$$\xi = \frac{x+y}{|C_I(\pm)|}\big(\mu^{(1)} + \mu^{(p)}\big) + \frac{x-y}{|C_I(\pm)|}\big(\mu^{(2)} + \mu^{(2p)}\big).$$

Since $\xi \in R$, we have $(x+y)/|C_I(\pm)|, (x-y)/|C_I(\pm)| \in \boldsymbol{Z}$. This implies that $R \cap \big(\boldsymbol{C} e_{\chi_{(0)}} + \boldsymbol{C} e_{\chi_{(2)}}\big)$ is contained in $\boldsymbol{Z}(\mu^{(1)} + \mu^{(p)}) + \boldsymbol{Z}(\mu^{(2)} + \mu^{(2p)})$. Conversely, let ξ be any element of $\boldsymbol{Z}(\mu^{(1)} + \mu^{(p)}) + \boldsymbol{Z}(\mu^{(2)} + \mu^{(2p)})$. Since $\mu^{(1)} + \mu^{(p)} = (p-1)\big(e_{\chi_{(0)}} + e_{\chi_{(2)}}\big)$ and $\mu^{(2)} + \mu^{(2p)} = (p-1)\big(e_{\chi_{(0)}} - e_{\chi_{(2)}}\big)$, we have $\xi \in \boldsymbol{C} e_{\chi_{(0)}} + \boldsymbol{C} e_{\chi_{(2)}}$. This completes the proof. □

We denote by $\mathscr{Z}$ the subgroup of R defined by

$$\mathscr{Z} = \boldsymbol{Z}\big(\mu^{(1)} + \mu^{(p)}\big) + \boldsymbol{Z}\big(\mu^{(2)} + \mu^{(2p)}\big). \tag{5.20}$$

As the element s mentioned above, we take the following one of $\mathscr{Z}$

$$s = \mu^{(1)} + \mu^{(p)}, \tag{5.21}$$

and put

$$\theta' = \theta_p - s. \tag{5.22}$$

Concerning the e_χ-components of s we have the following:

$$s = (p-1)\bigl(e_{\chi_{(0)}} + e_{\chi_{(2)}}\bigr). \tag{5.23}$$

The following proposition says that we can replace the index $[R_{0,0} : I_{12}\theta_p]$ in (5.18) by $[(R_{0,0} + \mathscr{Z}) : (I_{12}\theta' + \mathscr{Z})]$.

Proposition 5.5. *Let s, θ' and $\mathscr{Z}$ be as above. Then we have the following.*

(1) $Rs = \mathscr{Z}$.
(2) $R_{0,0} \cap \mathscr{Z} = 0$.
(3) $I_{12}\theta_p \subset I_{12}\theta' + \mathscr{Z}$.
(4) $R_{0,0} \cap \bigl(I_{12}\theta' + \mathscr{Z}\bigr) = I_{12}\theta_p$.
(5) $R_{0,0} + I_{12}\theta' + \mathscr{Z} = R_{0,0} + \mathscr{Z}$.
(6) $\bigl(R_{0,0} + \mathscr{Z}\bigr)/\bigl(I_{12}\theta' + \mathscr{Z}\bigr) \cong R_{0,0}/(I_{12}\theta_p)$.

Proof.

(1) Let ξ be any element of R. Then, $\xi s = \xi\mu^{(1)} + \xi\mu^{(p)} = \sum_{r\in T} \deg \xi^{(r)}\mu^{(r)} + \sum_{r\in T} \deg \xi^{(rop)}\mu^{(r)} = \sum_{r=1,p} \deg \xi^{(r)} \cdot \sum_{r=1,p} \mu^{(r)} + \sum_{r=2,2p} \deg \xi^{(r)} \cdot \sum_{r=2,2p} \mu^{(r)} \in \mathscr{Z}$, which implies $Rs \subset \mathscr{Z}$. Conversely, let $\xi = a(\mu^{(1)} + \mu^{(p)}) + b(\mu^{(2)} + \mu^{(2p)})$ with $a, b \in \boldsymbol{Z}$ be any element of $\mathscr{Z}$. Since $\mu^{(2)} + \mu^{(2p)} = [2]s$, we have $\xi = as + b[2]s = (a + b[2])s \in Rs$. This implies $\mathscr{Z} \subset Rs$. Hence, (1) is proved.

(2) This is obvious from the definition of $R_{0,0}$ and Lemma 5.1 because the e_χ-component is 0 for every character χ of $C_I(\pm)$.

(3) Let ξ be any element of I_{12}. Then $\xi\theta_p = \xi(\theta' + s) = \xi\theta' + \xi s$. Since $\xi s \in \mathscr{Z}$ by (1), this proves (3).

(4) By (1) of Proposition 5.4 and (3) above, we have $I_{12}\theta_p \subset R_{0,0} \cap (I_{12}\theta' + \mathscr{Z})$. Conversely, let η be any element of $R_{0,0} \cap (I_{12}\theta' + \mathscr{Z})$. Let us write $\eta = \xi\theta' + as + b[2]s$ with $\xi \in I_{12}$ and $a, b \in \boldsymbol{Z}$. Put $\eta_1 = \xi\theta_p$ ($\in I_{12}\theta_p$). Then $\eta_1 = \xi\theta' + \xi s = \xi\theta' + \bigl\{\sum_{r=1,p} \deg \xi^{(r)}\bigr\}s + \bigl\{\sum_{r=2,2p} \deg \xi^{(r)}\bigr\}[2]s$. Hence $\eta - \eta_1 = \bigl\{a - \sum_{r=1,p} \deg \xi^{(r)}\bigr\}s + \bigl\{b - \sum_{r=2,2p} \deg \xi^{(r)}\bigr\}[2]s \in \mathscr{Z}$. Since $\eta \in R_{0,0}$ by the assumption and $\eta_1 \in I_{12}\theta_p \subset R_{0,0}$, we have $\eta - \eta_1 \in R_{0,0} \cap \mathscr{Z}$. This implies $\eta = \eta_1$ by (2) above, whence $\eta \in I_{12}\theta_p$. We have, therefore, $R_{0,0} \cap (I_{12}\theta' + \mathscr{Z}) \subset I_{12}\theta_p$. This proves (4).

(5) It is sufficient to prove $I_{12}\theta' \subset R_{0,0} + \mathscr{Z}$. Let ξ be any element of I_{12}. Then $\xi\theta' = \xi\theta_p - \xi s$. Since $\xi\theta_p \in I_{12}\theta_p \subset R_{0,0}$ by (1) of Proposition 5.4 and $\xi s \in \mathscr{Z}$ by (1) above, we have $\xi\theta' \in R_{0,0} + \mathscr{Z}$. This proves (5).

(6) By (4) and (5) above, we have the following isomorphism

$$\begin{aligned}(R_{0,0} + \mathscr{Z})/(I_{12}\theta' + \mathscr{Z}) &= (R_{0,0} + I_{12}\theta' + \mathscr{Z})/(I_{12}\theta' + \mathscr{Z}) \\ &\cong R_{0,0}/\bigl\{R_{0,0} \cap (I_{12}\theta' + \mathscr{Z})\bigr\} = R_{0,0}/(I_{12}\theta_p),\end{aligned}$$

which proves (6). □

5.5. Extending $\boldsymbol{R_{0,0}} + \mathscr{X}$ to $\boldsymbol{R}$.

By (5.18) and (6) of Proposition 5.5 we have

$$\begin{aligned} h &= \frac{p^2-1}{24}[R_{0,0} : I_{12}\theta_p] \\ &= \frac{p^2-1}{24}\big[(R_{0,0}+\mathscr{X}) : (I_{12}\theta' + \mathscr{X})\big]. \end{aligned} \tag{5.24}$$

Here we consider the extension R of $R_{0,0} + \mathscr{X}$, and determine its index $[R : R_{0,0} + \mathscr{X}]$ in two steps. Let $R_{p-1,p-1}$ be the subgroup of R consisting of all elements ξ such that the following congruences hold (note that $\chi_{(0)}(\xi)$ and $\chi_{(2)}(\xi)$ are integers):

$$\chi_{(0)}(\xi) \equiv \chi_{(2)}(\xi) \equiv 0 \ (\mathrm{mod}(p-1)). \tag{5.25}$$

First we determine the index $[R_{p-1,p-1} : R_{0,0} + \mathscr{X}]$.

Proposition 5.6. *Let $R_{p-1,p-1}$ be as above. Then we have the following.*

(1) $R_{0,0} + \mathscr{X} \subset R_{p-1,p-1}$.
(2) $R_{p-1,p-1}/(R_{0,0} + \mathscr{X}) \cong \boldsymbol{Z}/2\boldsymbol{Z}$.

Proof.

(1) The inclusion $R_{0,0} \subset R_{p-1,p-1}$ is obvious by their definitions. By (5.23) we have $\chi_{(0)}(s) = \chi_{(2)}(s) = p-1$. Hence we have $\chi_{(0)}([2]s) = p-1$ and $\chi_{(2)}([2]s) = -(p-1)$. Since $\mathscr{X} = \boldsymbol{Z}s + \boldsymbol{Z}[2]s$, this implies $\mathscr{X} \subset R_{p-1,p-1}$, which proves (1).

(2) Let ξ be any element of $R_{p-1,p-1}$. Write $\chi_{(0)}(\xi) = a(p-1)$ and $\chi_{(2)}(\xi) = b(p-1)$ with $a, b \in \boldsymbol{Z}$. Let $\varphi(\xi)$ be the residue class of $a-b$ modulo 2. Then φ is a homomorphism from $R_{p-1,p-1}$ to $\boldsymbol{Z}/2\boldsymbol{Z}$. First we prove that φ is surjective. Put $\xi_1 = \mu^{(1)} + \mu^{(2)}$. Then $\chi_{(0)}(\xi_1) = p-1$ and $\chi_{(2)}(\xi_1) = 0$, which implies that $\xi_1 \in R_{p-1,p-1}$, and that $\varphi(\xi_1) = 1 (\mathrm{mod}\, 2)$. This proves the surjectivity of φ. Next we prove that the kernel of φ coincides with $R_{0,0} + \mathscr{X}$. By the definition of $R_{0,0}$ we have $\varphi(R_{0,0}) = 0$. By the values of $\chi_{(0)}(\xi)$ and $\chi_{(2)}(\xi)$ for $\xi = s$ and $[2]s$ in (1) above, we have $\varphi(s) = \varphi([2]s) = 0$. These imply that $R_{0,0} + \mathscr{X} \subset \varphi^{-1}(0)$. Conversely, let ξ be any element of $\varphi^{-1}(0)$, and write $\chi_{(0)}(\xi) = a(p-1)$, $\chi_{(2)}(\xi) = b(p-1)$ and $a - b = 2m$ with $a, b, m \in \boldsymbol{Z}$. Put $\xi_2 = \xi - \{(a-m)s + m[2]s\}$. Then we have

$$\begin{aligned} &\chi_{(0)}(\xi_2) = \chi_{(0)}(\xi) - (a-m)\chi_{(0)}(s) - m \cdot \chi_{(0)}([2]s) = 0, \\ &\chi_{(2)}(\xi_2) = \chi_{(2)}(\xi) - (a-m)\chi_{(2)}(s) - m \cdot \chi_{(2)}([2]s) = 0, \end{aligned}$$

which implies $\xi_2 \in R_{0,0}$. Since $(a-m)s+m[2]s \in \mathscr{X}$, we have $\xi \in R_{0,0}+\mathscr{X}$, hence $\varphi^{-1}(0) \subset R_{0,0}+\mathscr{X}$. This gives $\varphi^{-1}(0) = R_{0,0}+\mathscr{X}$, and completes the proof of (2). □

Next we determine the index $[R : R_{p-1,p-1}]$.

Proposition 5.7. *We have* $[R : R_{p-1,p-1}] = (1/2)(p-1)^2$.

Proof. Let ξ be any element of R. Let $\varphi(\xi)$ be the element of $(\boldsymbol{Z}/(p-1)\boldsymbol{Z})^2$ defined by

$$\varphi(\xi) = \big(\chi_{(0)}(\xi)(\mathrm{mod}(p-1)), \chi_{(2)}(\xi)(\mathrm{mod}(p-1))\big).$$

Then φ is a homomorphism from R to $(\boldsymbol{Z}/(p-1)\boldsymbol{Z})^2$. For each element $\alpha \in C_I(\pm)$, we have $\varphi(\alpha) = (1,1)$ or $(1,-1)$ according as $t(\alpha) = 1, p$ or $2, 2p$, respectively. This implies that the image $\operatorname{Im}\varphi$ of φ is the subgroup of $(\boldsymbol{Z}/(p-1)\boldsymbol{Z})^2$ generated by $(1,1)$ and $(1,-1)$. Since $(2,0) = (1,1)+(1,-1)$, $(0,2) = (1,1)-(1,-1)$, and $(1,-1) = (1,1)-(0,2)$, the group $\operatorname{Im}\varphi$ is generated by the three elements $(2,0)$, $(0,2)$ and $(1,1)$. Let A be the subgroup of $(\boldsymbol{Z}/(p-1)\boldsymbol{Z})^2$ generated by $(2,0)$ and $(0,2)$. Then, since $\operatorname{Im}\varphi \neq A$ and $2(1,1) \in A$, we have $[\operatorname{Im}\varphi : A] = 2$. Since $(2,0)$ and $(0,2)$ are independent and of order $(1/2)(p-1)$, we have $|A| = \{(1/2)(p-1)\}^2$, whence $|\operatorname{Im}\varphi| = 2\cdot\{(1/2)(p-1)\}^2 = (1/2)(p-1)^2$. Since $\varphi^{-1}(0) = R_{p-1,p-1}$, the proof is completed. □

5.6. The subgroup $\boldsymbol{I_{12}\theta'}$ of $\boldsymbol{I_{12}\theta'} + \mathscr{X}$.

In the equation (5.24) the group $I_{12}\theta' + \mathscr{X}$ appears. In this subsection we consider the subgroup $I_{12}\theta'$ of $I_{12}\theta'+\mathscr{X}$, and determine its index $[I_{12}\theta'+\mathscr{X} : I_{12}\theta']$.

Proposition 5.8. *We have the following.*

(1) $\mathscr{X} \cap I_{12}\theta' = (p-1)\mathscr{X}$.
(2) $(I_{12}\theta' + \mathscr{X})/I_{12}\theta' \cong (\boldsymbol{Z}/(p-1)\boldsymbol{Z})^2$.

Proof.

(1) By the definition (5.22) of θ', the e_χ-components of θ' are all non-zero, hence θ' is invertible in $R_{\boldsymbol{C}}$. In particular, since $\theta_p e_{\chi_{(0)}} = \theta_p e_{\chi_{(2)}} = 0$ (cf. Corollary 5.1), we have $\theta' e_{\chi_{(0)}} = -s e_{\chi_{(0)}}$ and $\theta' e_{\chi_{(2)}} = -s e_{\chi_{(2)}}$, hence $s(\theta')^{-1} e_{\chi_{(0)}} = -e_{\chi_{(0)}}$ and $s(\theta')^{-1} e_{\chi_{(2)}} = -e_{\chi_{(2)}}$. Since $s\big(e_{\chi_{(0)}} + e_{\chi_{(2)}}\big) = s$ by (5.23), we have $s(\theta')^{-1} = s(\theta')^{-1}\big(e_{\chi_{(0)}} + e_{\chi_{(2)}}\big) = -\big(e_{\chi_{(0)}} + e_{\chi_{(2)}}\big) = -(1/(p-1))s$. Let $\eta = as + b[2]s$ be any element of $\mathscr{X}$ $(a, b \in \boldsymbol{Z})$. Then we have

$$\eta(\theta')^{-1} = (a+b[2])s(\theta')^{-1} = -\frac{1}{p-1}(a+b[2])s = -\frac{1}{p-1}\eta. \tag{5.26}$$

Now let η be any element of $\mathscr{X}\cap I_{12}\theta'$, and write $\eta = as+b[2]s = \xi\theta'$ with $a, b \in \boldsymbol{Z}$ and $\xi \in I_{12}$. Then by (5.26) we have $\xi = \eta(\theta')^{-1} = -(a/(p-1))s - b/(p-1)[2]s$. Since $\xi \in R$, both the numbers $a/(p-1)$ and $b/(p-1)$ are integers. This implies that $a, b \in (p-1)\boldsymbol{Z}$ and that $\eta \in (p-1)\mathscr{X}$, namely $\mathscr{X}\cap I_{12}\theta' \subset (p-1)\mathscr{X}$. Conversely, let η be any element of $(p-1)\mathscr{X}$. Then by (5.26) we have $\eta(\theta')^{-1} \in \mathscr{X}$. We can verify by elementary calculations that both the elements s and $[2]s$ satisfy the congruence (i*) in (5.5) and the congruences (ii)–(iv) of Theorem 5.1. This implies that the elements s and $[2]s$ are contained in I_{12}, and hence $\mathscr{X} \subset I_{12}$. Put $\xi = \eta(\theta')^{-1}$. Then we have $\eta = \xi\theta' \in I_{12}\theta'$, which implies that $(p-1)\mathscr{X} \subset \mathscr{X}\cap I_{12}\theta'$. This proves (1).

(2) By (1) we have $(I_{12}\theta' + \mathscr{X})/I_{12}\theta' \cong \mathscr{X}/(\mathscr{X}\cap I_{12}\theta') = \mathscr{X}/(p-1)\mathscr{X}$. Since s and $[2]s$ is a basis of $\mathscr{X}$, we have $\mathscr{X}/(p-1)\mathscr{X} \cong (\boldsymbol{Z}/(p-1)\boldsymbol{Z})^2$. This proves (2). □

5.7. The cuspidal class number.

By (2) of Proposition 5.6 and Proposition 5.7, we have $[R : R_{0,0} + \mathscr{X}] = (p-1)^2$. Also, by (2) of Proposition 5.8, we have $[I_{12}\theta' + \mathscr{X} : I_{12}\theta'] = (p-1)^2$. Combining these equalities with (5.24), we have

$$\begin{aligned} h &= \frac{p^2-1}{24}\big[(R_{0,0} + \mathscr{X}) : (I_{12}\theta' + \mathscr{X})\big] \\ &= \frac{p^2-1}{24}\cdot\frac{1}{(p-1)^4}\big[R : I_{12}\theta'\big]. \end{aligned} \tag{5.27}$$

Let A and B be two lattices of $R_{\boldsymbol{Q}}$, and let C be a lattice contained in $A \cap B$. Then the quotient $[A : C]/[B : C]$ does not depend on the choice of C. We denote this number by $[A : B]$. It satisfies the usual multiplicative property, namely $[A : B] = [A : D][D : B]$. In particular, we have $[R : I_{12}\theta'] = [R : R\theta'][R\theta' : I_{12}\theta']$. Since θ' is invertible, we have $[R\theta' : I_{12}\theta'] = [R : I_{12}]$. By these equalities and (5.27) we have

$$h = \frac{p^2-1}{24}\cdot\frac{1}{(p-1)^4}[R : R\theta'][R : I_{12}]. \tag{5.28}$$

We determine the values $[R : I_{12}]$ and $[R : R\theta']$.

Proposition 5.9. *We have* $[R : I_{12}] = 48p^2$.

Proof. Let ξ be any element of R. Let $\varphi_1(\xi)$ be the element of $\boldsymbol{Z}/12\boldsymbol{Z}$ defined by the expression on the left-hand side of (i*) in (5.5). Let $\varphi_2(\xi)$ be the element of $\boldsymbol{Z}/4\boldsymbol{Z}$ defined by the expression on the left-hand side of (ii) in Theorem 5.1. Similarly, let $\varphi_3(\xi)$ (respectively $\varphi_4(\xi)$) be the element of $\boldsymbol{Z}/p\boldsymbol{Z}$ defined by the expression on the left-hand side of (iii) (respectively (iv)) in Theorem 5.1. Then $\varphi = (\varphi_1, \varphi_2, \varphi_3, \varphi_4)$ is a homomorphism from R to $\boldsymbol{Z}/12\boldsymbol{Z} \times \boldsymbol{Z}/4\boldsymbol{Z} \times \boldsymbol{Z}/p\boldsymbol{Z} \times \boldsymbol{Z}/p\boldsymbol{Z}$. The kernel of φ is I_{12}. We prove that φ is surjective. Put $\xi_1 = 7px \cdot 1_2 - 3px[2]$, where x is an integer such that $px \equiv 1 \pmod{12}$. Then we have $\varphi(\xi_1) = (1, 0, 0, 0)$. Put $\xi_2 = 6px \cdot 1_2 + 3px[2]$, where x is the same integer as in ξ_1. Then $\varphi(\xi_2) = (0, 1, 0, 0)$. Put $\xi_3 = 12y \cdot 1_2$, where y is an integer such that $12y \equiv 1 \pmod{p}$. Then $\varphi(\xi_3) = (0, 0, 1, 0)$. Put $\xi_4 = 12y[2p]$, where y is the same integer as in ξ_3. Then $\varphi(\xi_4) = (0, 0, 0, 1)$. This proves that φ is surjective, and hence the proof is completed. □

Proposition 5.10. *We have the following equation*

$$[R : R\theta'] = \frac{(p-1)^4}{48} \prod_{\psi} \left\{ (4 - \psi(2))^2 \left(\frac{1}{4} B_{2,\psi} \right)^4 \right\},$$

where ψ runs through all even, primitive Dirichlet characters modulo p.

Proof. Let $f : R_{\boldsymbol{Q}} \to R_{\boldsymbol{Q}}$ be the linear transformation on the vector space $R_{\boldsymbol{Q}}$ over $\boldsymbol{Q}$ defined by the multiplication by θ'. Let $\{x_i\}$ be a basis of R over $\boldsymbol{Z}$. Let $M(f)$ be the matrix of f determined by $\{x_i\}$. Then we have $[R : R\theta'] = |\det M(f)|$ by the theory of elementary divisor and the definition of $[R : R\theta']$. Since $\theta' e_\chi = \chi(\theta') e_\chi$ for any character χ of $C_I(\pm)$ and the set $\{e_\chi\}$ is a basis of $R_{\boldsymbol{C}}$ over $\boldsymbol{C}$, we have $\det M(f) = \prod_\chi \chi(\theta')$ where χ runs through all characters of $C_I(\pm)$. Let χ be a character of $C_I(\pm)$. Then, by the definition (5.22) of θ', Proposition 5.1 and (5.23), we have

$$\chi(\theta') = \frac{1}{4}(2 + \chi([2])) B_{2,\overline{\psi}}, \tag{5.29}$$

where $\psi = \psi_\chi$, if χ is non-trivial on $C_I^{(1)}(\pm)$. When χ is trivial on $C_I^{(1)}(\pm)$, it is one of $\chi_{(0)}$, $\chi_{(2)}$, $\chi_{(p)}$ or $\chi_{(2,p)}$, and we have

$$\chi(\theta') = \begin{cases} -(p-1) & \text{if } \chi = \chi_{(0)} \text{ or } \chi_{(2)}, \\ -\dfrac{1}{4}(p-1) & \text{if } \chi = \chi_{(p)}, \\ -\dfrac{1}{12}(p-1) & \text{if } \chi = \chi_{(2,p)}. \end{cases} \tag{5.30}$$

Let ψ be a non-trivial, even character of $(\boldsymbol{Z}/p\boldsymbol{Z})^\times$. Then the set of characters χ of $C_I(\pm)$ with $\psi_\chi = \psi$ consists of four elements. Let χ be anyone of them. Then the other characters are $\chi\chi_{(2)}$, $\chi\chi_{(p)}$ and $\chi\chi_{(2,p)}$. Put $\chi_0 = \chi_{(0)}$, $\chi_1 = \chi_{(2)}$, $\chi_2 = \chi_{(p)}$ and $\chi_3 = \chi_{(2,p)}$. We prove that

$$\prod_{i=0}^{3} \big(2 + (\chi\chi_i)([2])\big) = (4 - \psi(2))^2. \tag{5.31}$$

In fact, since $\chi_0([2]) = \chi_2([2]) = 1$ and $\chi_1([2]) = \chi_3([2]) = -1$, the left-hand side of (5.31) is equal to

$$\left\{4 - \chi([2])^2\right\}^2 = \left\{4 - \chi([2]^2)\right\}^2. \tag{5.32}$$

By the definition of [2] (cf. (2.45)), the element $[2]^2$ is an element of $C_I^{(1)}(\pm)$ represented by the matrix $(2+p)1_2$. Hence we have $\chi([2]^2) = \psi(2)$, which proves (5.31). Now, by (5.31) and (5.29), we have

$$\prod_{i=0}^{3} (\chi\chi_i)(\theta') = (4 - \psi(2))^2 \left(\frac{1}{4} B_{2,\overline{\psi}}\right)^4. \tag{5.33}$$

On the other hand, for four characters which are trivial on $C_I^{(1)}(\pm)$, we have

$$\prod_{i=0}^{3} \chi_i(\theta') = \frac{1}{48}(p-1)^4 \tag{5.34}$$

by (5.30).

Since the product of (5.33) with ψ ranging over all even, primitive Dirichlet characters modulo p coincides with the product $\prod_\chi \chi(\theta')$ with χ non-trivial on $C_I^{(1)}(\pm)$, we have, by this and (5.34),

$$\begin{aligned}\prod_{\chi}\chi(\theta') &= \frac{(p-1)^4}{48}\prod_{\psi}\left\{(4-\psi(2))^2\left(\frac{1}{4}B_{2,\overline{\psi}}\right)^4\right\}\\ &= \frac{(p-1)^4}{48}\prod_{\psi}\left\{(4-\psi(2))^2\left(\frac{1}{4}B_{2,\psi}\right)^4\right\}, \qquad (5.35)\end{aligned}$$

where χ runs through all characters of $C_I(\pm)$. Since the value of the right-hand side of (5.35) is a positive real number, combining the equality (5.35) with the relation $[R : R\theta'] = |\det M(f)| = |\prod_{\chi}\chi(\theta')|$, we have the proof. □

By (5.28) and Propositions 5.9–5.10, we have the following formula for the cuspidal class number.

Theorem 5.2. *Let p be a prime $\neq 2, 3$. Let h be the cuspidal class number of the modular curve $X_1(2p)$. Then we have*

$$h = \frac{p^2-1}{24}\cdot p^2\cdot\prod_{\psi}\left\{(4-\psi(2))^2\left(\frac{1}{4}B_{2,\psi}\right)^4\right\},$$

where ψ runs through all even, primitive Dirichlet characters modulo p.

References

[1] A. Agashe, Rational torsion in elliptic curves and the cuspidal subgroup, preprint, arXiv:math/0810.5181, 2008.

[2] Y. Chen, Cuspidal ***Q***-rational torsion subgroup of $J(\Gamma)$ of level p, Taiwanese J. Math., **15** (2011), 1305–1323.

[3] B. Conrad, B. Edixhoven and W. Stein, $J_1(p)$ has connected fibers, Doc. Math., **8** (2003), 331–408.

[4] V. G. Drinfeld, Two theorems on modular curves, Funct. Anal. Appl., **7** (1973), 155–156.

[5] S. Klimek, Thesis, Berkeley, 1975.

[6] D. Kubert, The square root of the Siegel group, Proc. London Math. Soc. (3), **43** (1981), 193–226.

[7] D. Kubert and S. Lang, Modular Units, Grundlehren der Mathematischen Wissenschaften, **244**, Springer-Verlag, Berlin, 1981.

[8] J. Manin, Parabolic points and zeta functions of modular curves, Izv. Akad. Nauk SSSR Ser. Mat., **36** (1972), 19–64.

[9] B. Mazur, Modular curves and the Eisenstein ideal, Inst. Hautes Études Sci. Publ. Math., **47** (1977), 33–186.

[10] A. Ogg, Rational points on certain elliptic modular curves, AMS Conference, St. Louis, 1972, pp. 211–231.

[11] A. Ogg, Diophantine equations and modular forms, Bull. Amer. Math. Soc., **81** (1975), 14–27.

[12] G. Stevens, The cuspidal group and special values of L-functions, Trans. Amer. Math.

Soc., **291** (1985), 519–550.

[13] T. Takagi, Cuspidal class number formula for the modular curves $X_1(p)$, J. Algebra, **151** (1992), 348–374.

[14] T. Takagi, The cuspidal class number formula for the modular curves $X_1(p^m)$, J. Algebra, **158** (1993), 515–549.

[15] T. Takagi, The cuspidal class number formula for the modular curves $X_1(3^m)$, J. Math. Soc. Japan, **47** (1995), 671–686.

[16] T. Takagi, The cuspidal class number formula for the modular curves $X_0(M)$ with M square-free, J. Algebra, **193** (1997), 180–213.

[17] T. Takagi, The cuspidal class number formula for the modular curves $X_1(2^{2n+1})$, J. Algebra, **319** (2008), 3535–3566.

[18] T. Takagi, Modified Siegel functions relative to the principal congruence subgroups of $G(\sqrt{M})$, J. Faculty of Arts and Sciences at Fujiyoshida, Showa University, **4** (2009), 1–16.

[19] T. Takagi, The cuspidal class number formula for certain quotient curves of the modular curve $X_0(M)$ by Atkin-Lehner involutions, J. Math. Soc. Japan, **62** (2010), 13–47.

[20] Y. Yang, Modular units and cuspidal divisor class groups of $X_1(N)$, J. Algebra, **322** (2009), 514–553.

[21] J. Yu, A cuspidal class number formula for the modular curves $X_1(N)$, Math. Ann., **252** (1980), 197–216.

Toshikazu Takagi
Faculty of Arts and Sciences at Fujiyoshida
Showa University
Fujiyoshida
Yamanashi 403-0005, Japan
E-mail: takagi@cas.showa-u.ac.jp